1-19-2016

It's More Than Just Changing Your Password: Exploring the Nature and Antecedents of Cyber-Security Behaviors

Rachel Christine Dreibelbis

It's More Than Just Changing Your Password:

Exploring the Nature and Antecedents of Cyber-Security Behaviors

by

Rachel C. Dreibelbis

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts
Department of Psychology
College of Arts and Sciences
University of South Florida

Major Professor: Michael D. Coovert, Ph.D.
Walter Borman, Ph.D.
Joseph Vandello, Ph.D.

Date of Approval:
February 26, 2016

Keywords: cyberpsychology, insider threat, personality, organizational citizenship behaviors, counterproductive work behaviors

Dedication

This thesis is dedicated in loving memory of my father, Ron Dreibelbis. Before his passing he supported and inspired me with unconditional love, support, and wisdom in all of my pursuits. It is also dedicated to my mother, Lisa Dreibelbis, who continues to be my number one fan and supporter throughout this process. Lastly, it is dedicated to my best friend, Paige Lake, who never fails to encourage and motivate me throughout my graduate school career.

Acknowledgments

I would like to thank Dr. Mike Coovert, who provided invaluable feedback and guidance throughout all stages of this project. I am grateful for everything he has done for me as my advisor and mentor. I would also like to thank the members of my committee, Dr. Wally Borman and Dr. Joe Vandello, for all their guidance and assistance. Finally, I thank Jackie Martin for her support and feedback on multiple iterations of this project.

Table of Contents

List of Tables

List of Figures

Abstract

Organizations have become increasingly concerned with developing and protecting their information security systems. Despite attempts to secure the information infrastructure, employees inside of organizations remain the largest source of threat to information cyber-security. While previous research has focused on behavioral and situational factors that influence cyber-security behaviors, the measurement of cyber behaviors and their relationship to other performance variables is poorly understood. The purpose of the present study is to 1) determine the underlying factor structure of a cyber-security behavior scale, 2) assess if individual personality traits predict four types of cyber-security behaviors: security assurance, security compliance, security risk, and security damaging behaviors, and 3) explore the relationship between citizenship and counterproductive work behaviors and cyber-security behaviors. Results indicate that cyber-security behavior can be separated into four distinct dimensions and that personality traits such as conscientiousness, agreeableness, and openness to experience are predictive of these behaviors. Additionally, positive cyber behaviors are related organizational citizenship behaviors, and potentially harmful cyber behaviors related to counterproductive work behaviors. This research has implications for using personality to predict cyber-security behaviors and reduce insider threat in the workplace.

Chapter One
Introduction

In an increasingly digital age, organizations continue to acquire more digital assets and move their information and communications to online networks. With this shift in information location comes a new kind of threat: cyber-security. Instead of a concern for information loss through the theft of physical files, organizations face the potential loss of information and assets via the cyber world, be it through internal or external sources. In the face of evolving technology and imminent threats to information, organizations find it increasingly difficult predict the types of risks they may face (Pfleeger & Caputo, 2012; Warkentin & Willison, 2009). Organizations implement security systems through various technologies to ensure that their information is protected against attackers and other organizations, however even the most intensive security measures can be compromised if the organization's employees are behaving in such a way that poses risks to information cyber-security.

Past research shows that internally-based threats (i.e. employees, insiders) are at present the largest threat to an organization's information (e.g. Hu, Dinev, Hart, & Cooke, 2012; Stanton et al., 2005; Van Kessel, 2008; Warkentin & Willison, 2009), and employee actions make up the primary reason for losses of company information (CSI computer crime and security survey, as cited in Hu et al., 2012). In fact, 59% of past employees have admitted to stealing confidential information from their organization (Symantec & Ponemon, 2009). In the current study, the term "employee" refers to both end users and information technology employees. End users view an organization's information systems as a mechanism to perform work-related responsibilities,

while IT employees are responsible for overseeing those systems. Both groups are included because both have the potential to help or harm the organization via the information security systems. Organizational cyber-security infrastructure must not only ensure the stability of a company's hardware and software protection, but also strive to create a workforce that promotes positive cyber-security habits and prohibits behaviors that could put an organization at risk in the cyber realm.

Consequently, employees' cyber-security behaviors have recently drawn much attention from scholars, and as such, behaviors have direct implications for security in organizations. Past research suggests that many factors such as: organizational norms, security awareness, motivation, leadership, and organizational culture; affect an employee's propensity to engage in actions that could either protect an organization's digital information or put it at risk (Guo et al., 2011; Guo et al., 2013; Hu et al., 2012; Padayachee, 2012). As an alternative to demonstrating factors that influence these current employee cyber-security behaviors, organizations with special concerns for protecting their digital information may be able to proactively select employees who will engage in behaviors to protect the organization's digital assets. Using personality to identify these individuals is one option for organizations, and has not been explored fully in previous research, though it may prove an important avenue in the cyber-security realm. This research seeks to fill that gap, and open a new line of research into the selection of "cyber-security champions." Additionally, it remains unclear if cyber behaviors are merely forms of citizenship and counterproductive work behaviors, or if they are distinct work behaviors that should be studied as such. This thesis seeks to understand the factor structure underlying cyber-security behaviors, identify personality characteristics that are associated with these behaviors, and explore the relationship between these behaviors and organizational

citizenship and counterproductive work behaviors. The primary purposes of this study are to 1) analyze the underlying factor structure of a new cyber-security scale, 2) investigate the relationships between cyber-security behaviors, personality, organizational citizenship behaviors, and counterproductive work behaviors.

Defining Cyber-Security Behaviors

Scholars have noted that there is much disagreement about how cyber-security behaviors are best conceptualized (Guo, 2013). See Table 1 for a summary of the taxonomies discussed in the following section. Some studies have emphasized predicting and identifying positive cyber behaviors, while others focus on predicting negative behaviors. This method of research, however, may be problematic because antecedents of positive behaviors, like policy compliance, may be inherently distinct from antecedents of negative, risky cyber behaviors. Loch, Carr, and Warkentin (1992) defined a four-dimensional model of threats, such that the type of threat depends on the source (internal or external), perpetrator (human or non-human), intention (intentional or accidental), and consequences (disclosure of information, modification, destruction, or denial of service). Similarly, Im and Baskerville (2005) stated that threats caused by people are either accidental or deliberate. They further clarified that deliberate threats involve two components: mode and motive. Modes of carrying out the threat involve physical assault of the system, falsification, malicious code, and cracking of the security infrastructure. Motive can be fraud, espionage, or vandalism (Im & Baskerville, 2005).

Stanton, Stam, Mastrangelo, and Jolton (2005) adopted a two-factor taxonomy of end user security behaviors: user expertise and user intentions. Every cyber-security behavior performed by employees involves some amount of technical expertise on the employee's part, ranging from little expertise to expert knowledge of computers and software systems. The second

dimension, user intentions, captures the intentionality of the behaviors, ranging from benevolent to malicious intentions (Stanton et al., 2005). Based on interviews conducted with information security technology professionals, managers, and regular employees, they defined six categories of cyber-security behaviors arranged along the two dimensions of expertise and intentions (Stanton et al., 2005). These six categories include intentional destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware assurance, and basic hygiene (Stanton et al, 2005).

Intentional destruction behavior involves a relatively high level of expertise paired with intentions to harm the organization's information infrastructure. An example of such a behavior would be an employee who breaks into an organization's protected files to steal information (Stanton et al., 2005). Detrimental misuse does not require a high level of technical expertise, but still includes an intention of harm, possibly through "annoyance, harassment, rule breaking etc." (Stanton et al., 2005, p. 126). For example, an employee might use the company email to send spam to market a sideline business. Dangerous tinkering, unlike intentional destruction and detrimental misuse, does not involve a clear intention of harm. These behaviors require technical expertise and an example of such a behavior involves an employee who "configures a wireless gateway that inadvertently allows wireless access to the company's network by people in passing cars" (Stanton et al., 2005, p. 126). Naïve mistakes require minimal expertise and no intention to do harm, however these actions still pose a potential risk to the organization. For example, an employee might choose an insecure password for their computer, such as "password" or their birthday.

Aware assurance and basic hygiene behaviors tend to help the organization and are viewed as behaviors that the organization seeks to promote. Aware assurance behaviors involve a high level of expertise combined with the intentions of protecting the organization's information

technology. An example of such a behavior would be an employee who, by monitoring of their work computer, recognizes the presence of a backdoor program that would allow illegal access to the information on their computer. Lastly, basic hygiene behaviors require little expertise but include a clear intention to protect, and would involve an employee who refuses to reveal their password to an unknown caller claiming to be from computer services. By creating these categories, Stanton et al. (2005) were able to organize specific behaviors into a manageable taxonomy. They specifically clarify that individuals who engage in one type of behavior may also engage in other types of behaviors. This taxonomy may help with assessing security related behaviors, and provides a useful framework for further classifying specific behaviors into broader categories in order to more manageably identify employees who tend to practice different cyber-security behaviors.

Seeing the need for further reconceptualization of cyber-related behaviors, Guo (2013) organized a new framework based on dimensions used in the current cyber literature. Guo (2013) used five dimensions: intentionality, motive, expertise, job relatedness, and consequence. Guo (2013) suggested that employees intentionally or unintentionally engage in a given behavior, may have malicious or non-malicious motive, and may have varying degrees of information technology expertise. Additionally, some behaviors may be more related to an employee's job than others. Lastly, employee cyber-related behaviors can have a range of consequences for the organization, ranging from improved security to direct damage to the organization.

Using those dimensions, Guo (2013) classified information security-related behavior into four categories: security assurance behaviors (SABs), security compliant behaviors (SCBs), security risk-taking behaviors (SRBs), and security damaging behaviors (SDBs). According to Guo (2013) these categories are designed to be distinct from each other, meaning that factors

influencing these behaviors may be inherently different and should be studied with this in mind. Ideally, organizations want to promote SABs and SCBs while preventing SRBs and SDBs.

Security Assurance Behaviors

SABs are behaviors in which an employee has clear intent to help protect an organization's information security (Guo, 2013). SABs are effortful, benevolent actions on the part of the employee, and typically involve going above and beyond what is required by the organization in order to protect information security. Like Stanton et al's (2005) aware assurance and basic hygiene behaviors, Guo (2013) suggests that employees need a high level of technological expertise (e.g. identifying a virus), though it can be argued that there are simpler actions, like choosing a strong password and monitoring your computer for signs of a virus, which can be performed by any end user. These behaviors may be related to organizational citizenship behaviors (Organ, 1988) because they are benevolent in nature and demonstrate a desire to help the organization.

Security Compliance Behaviors

SCBs are "behaviors that are in line with organizational security policies" (Guo, 2013, p. 248). While SABs are deliberate behaviors, SCBs may be a result of action or inaction. Employees might simply be following information security rules or not engaging in risky or damaging behavior. Past research has identified extrinsic and intrinsic motivational factors that may influence compliant behaviors, but not personality factors (Padayachee, 2012). Padayachee (2012) notes, however, that certain personality traits could contribute to an employee's sense of personal conduct and should be a focus of future research. Antecedents of compliance intention include employee past behavior, severity and certainty of punishment, organizational norms and

peer behavior, and the extent to which their compliance is effective for organizational information security (Herath & Rao, 2009; Vance, Siponen, & Pahnila, 2012).

Security Risk Behaviors

SRBs are "behaviors that may put the organization's information security at risk" and involve actions in which employees "do what they are expected not to do" (Guo, 2013, p. 248-249). Employees engaging in these behaviors might not intend to harm the organization, but rather may view these behaviors as convenient for getting their job done (Guo, 2013). Regardless, any risk behavior may have negative consequences for the organization. Employees with any level of technological expertise can perform these behaviors. Some examples of SRBs could include walking away from your computer without locking it first, or writing down a work password where others might see it. SRBs are conceptually similar to Stanton et al.'s (2005) naïve mistakes and dangerous tinkering behaviors and non-malicious security violations (NSMV) as defined by Guo, Yuan, Archer, and Connelly (2011). Guo et al. (2011) showed that employee intentions to perform NSMVs are higher if they believe that doing so will improve their job performance.

Security Damaging Behaviors

SDBs are behaviors that organizations prohibit employees from doing and will cause damage to the organization's information security. These behaviors are generally malicious in nature and can result in disciplinary action both by the organization and government. SDBs are generally considered to be more severe than SRBs. These behaviors may require a high level of technological expertise on the part of the employee and could be considered similar in nature to organizationally directed counterproductive work behaviors (Robinson & Bennett, 1995).

For the purposes of the present study, Guo's (2013) taxonomy of cyber-security behaviors are used as the basis for scale creation. Using these four categories of behavior as a framework, items describing each behavior are tested to determine the underlying factor structure of behaviors. This will allow researchers to measure these behaviors and utilize the scale for future use in predicting and evaluating these behaviors in the workplace.

Factor Structure of Cyber Behaviors

The first goal of this thesis is to determine the nature of cyber-security behaviors. As discussed earlier, previous research has classified cyber behaviors along several different taxonomies (i.e. Guo, 2013; Lock et al., 1992; Stanton et al., 2005), but little has been done to determine the factor structure underlying these behaviors. Although studies in the information security context frequently measure behavioral intentions, rather than actual behaviors, it is preferable to measure the latter rather than the former. Even though there is a link between intentions and behavior, intentions do not always lead to behaviors. This is especially troubling because it only takes one risky behavior to put an organization's information in jeopardy (Crossler et al., 2013). For this reason, the current study intends to assess the frequency of cyber-security behaviors, using a 23-item measure covering security assurance, compliance, risk, and damaging behaviors. Because past research in cyber-security focuses primarily on behavioral intentions from a single type of security behavior, no single measure adequately covers behaviors from all four areas. This thesis will not only determine the structural nature of the data to determine if the data fits a four factor model, but also validate a scale aims to provide a foundation of measurement for these behaviors.

Research Question 1: What is the underlying factor structure of cyber-security behaviors?

Personality

For many years, researchers have attempted to define and organize personality traits for personnel selection purposes (Barrick & Mount, 1991). Trait theory is arguably the best way to study personality (Korzaan & Boswell, 2005; McCrae & Costa, 2012). A widely accepted taxonomy of personality is the Five Factor Model, with origins from McDougall (1932), who stated, "personality may with advantage be broadly analyzed into five distinguishable but inseparable factors, namely, intellect, character, temperament, disposition, and temper" (p.15). Norman (1963) later labeled the five factors extraversion, emotional stability, agreeableness, contentiousness, and culture based on the work of Fiske (1949), who found that data fit a five factor model well. McCrae and Costa (1985, 1987) confirmed this framework of a five factor model. Norman's (1963) five factors are commonly known as the "Big Five". The Big Five factors have been shown to be independent of cognitive ability (McCrae & Costa, 1987). Though there has been some debate about the definition about each other factors (Barrick & Mount, 1991), some common terms used to describe each factor are presented below.

Extraversion

Extraversion involves interpersonal tendencies, and is associated with traits such as sociability, gregariousness, assertiveness, talkativeness, and activeness (Barrick & Mount, 1991). It has also been defined using facets of enthusiasm and assertiveness (DeYoung, 2006; DeYoung, Quilty, Peterson, 2007).

Emotional Stability

Emotional Stability (Neuroticism) is a generally agreed upon dimension (Barrick & Mount, 1991). It involves emotional adjustment, and includes facets such as anxiety, anger,

embarrassment, worry, insecurity, vulnerability, impulsiveness, volatility, withdrawal (Barrick & Mount, 1991; DeYoung, 2006; DeYoung, Quilty, Peterson, 2007).

Agreeableness

Agreeableness also involves interpersonal tendencies, and reflects concern for cooperation and social harmony. Facets include; cooperation, compassion, forgiving, modesty, lack of hostility, nurturance, politeness, trust, and tolerance (Barrick & Mount, 1991; DeYoung, 2006; DeYoung, Quilty, Peterson, 2007). This dimension is often associated with prosocial elements (Chiaburu, Oh, Berry, Li, & Gardner, 2011).

Conscientiousness

Though there is some debate about the label, it has been defined as involving dependability, being careful, thorough, responsible, organized, and planful (Barrick & Mount, 1991), as well as the tendency to be self-disciplined.

Openness to Experience

Openness to Experience has also be called Culture (Norman, 1963). Traits associated with this factor include imaginative, cultured, curious, original, broad-minded, intelligent, and artistically sensitive (Barrick & Mount, 1991).

Personality and Cyber Behaviors

Do certain personality traits predict relevant cyber-security behaviors? The second goal of this thesis is to determine if personality traits are related to these behaviors. Given that cyber-security behavior research is a relatively new area of exploration, little has been done to examine the relationship between personality variables and different cyber-security related behaviors in organizations. While personality is more distal than situational variables, identifying those traits that predict cyber behaviors can aid organizations in selecting individuals who will engage in

compliance and assurance behaviors, rather than simply relying on training after hire. The present study investigates the predictive ability of the Big Five personality dimensions on the four types of cyber-security related behaviors as defined by Guo (2013).

I hypothesize that conscientiousness, agreeableness, and openness to experience will be valid predictors of security assurance behaviors (SABs). Chiaburu et al. (2011) found that conscientiousness, agreeableness, and openness to experience are the strongest predictors of organizationally directed Organizational Citizenship behaviors, probably due to the prosocial nature of the items in the measure. Conscientiousness is expected to be positively related to SABs because it involves prosocial characteristics, and conscientious individuals possess the desire to protect the organization. Thus, highly conscientious individuals would go the "extra step" to ensure that work information is secure. Agreeableness is expected to be positively related to SABs. Similar to conscientiousness, agreeableness is related to prosocial characteristics and thus may contribute to a desire to help and protect the organization. Lastly, openness to experience will predict SABs. Barrick & Mount (1991) found that openness to experience is related to training performance, so those high on this trait may be more receptive to information security training, and act out those trained behaviors to protect the organization's information security.

Hypothesis 1a: Conscientiousness will be positively related to security assurance behaviors.

Hypothesis 1b: Conscientiousness will predict security assurance behaviors, such that individuals high in conscientiousness will engage in more security assurance behaviors than individuals low in conscientiousness.

Hypothesis 1c: Agreeableness will be positively related to security assurance behaviors.

Hypothesis 1d: Agreeableness will predict security assurance behaviors, such that individuals high in agreeableness will engage in more security assurance behaviors than individuals low in agreeableness.

Hypothesis 1e: Openness to Experience will be positively related to security assurance behaviors.

Hypothesis 1f: Openness to Experience will predict security assurance behaviors, such that individuals high in openness to experience will engage in more security assurance behaviors than individuals low in openness to experience.

Conscientiousness will be related to SCBs, as past research has shown that conscientiousness is related to rule-following behavior (Hu et al., 2012). Hu et al. (2012) found that dutifulness was positively related to information security compliance intentions, which is a facet of conscientiousness. Individuals high in conscientiousness will have a high propensity to follow organizational policy, thus engaging in security compliance behaviors.

Hypothesis 2a: Conscientiousness will be positively related to security compliance behaviors.

Hypothesis 2b: Conscientiousness will predict security compliance behaviors, such that individuals high in conscientiousness will engage in more security compliance behaviors than individuals low in conscientiousness.

I hypothesize that conscientiousness will predict security risk behaviors. Conscientiousness will be negatively related to risk behaviors, since individuals low in conscientiousness will be more willing to engage in risk behaviors because they will be less likely to take the consequences of such behaviors into consideration.

Hypothesis 3a: Conscientiousness will be negatively related to security risk behaviors.

Hypothesis 3b: Conscientiousness will predict security risk behaviors, such that individuals low in conscientiousness will engage in more security risk behaviors than individuals high in conscientiousness.

I predict that emotional stability, agreeableness, and conscientiousness will predict security damaging behaviors (SDBs). Berry, Ones, and Sackett (2007) found that these three traits relate to organizational deviance, and I expect a similar relationship to these traits and SDBs, given the nature of these damaging behaviors. Individuals low in emotional stability may be volatile and impulsive, increasing the propensity to engage in damaging behaviors. Similarly, individuals low in agreeableness and conscientiousness may have a tendency to be hostile and lack need for cooperation and self-discipline, making damaging behaviors more likely.

Hypothesis 4a: Conscientiousness will be negatively related to security damaging behaviors.

Hypothesis 4b: Conscientiousness will predict security damaging behaviors, such that individuals low in conscientiousness will engage in more security damaging behaviors than individuals high in conscientiousness.

Hypothesis 4c: Agreeableness will be negatively related to security damaging behaviors.

Hypothesis 4d: Agreeableness will predict security damaging behaviors, such that individuals low in agreeableness will engage in more security damaging behaviors than individuals high in agreeableness.

Hypothesis 4e: Emotional Stability will be negatively related to security damaging behaviors.

Hypothesis 4f: Emotional Stability will predict security damaging behaviors, such that individuals low in emotional stability will engage in more security damaging behaviors than individuals high in emotional stability.

Organizational Citizenship Behaviors

Organizational citizenship behaviors, alternatively known as contextual performance, (Borman & Motowidlo, 1993) or extra-role behaviors (Van Dyne, Cummings, & Parks, 1995) were defined by Organ (1988) as "individual behavior that is discretionary, not directly or explicitly recognized by the formal reward system and that in aggregate promotes the effective functioning of the organization" (p. 4). This definition has been criticized by more recent research because OCBs are often viewed as a requirement by supervisors and related to performance evaluations, and thus, reward systems (Organ, 1997; Podsakoff, Whiting, Podsakoff, & Blume, 2009). Smith, Organ, and Near (1983) conceptualized OCBs as altruism and compliance behaviors, while Borman and Motowidlo (1993) expanded the criterion domain to a five-dimension taxonomy: persisting with enthusiasm, volunteering to carry out non-role tasks, helping and cooperating with others, following organizational rules and procedures, and endorsing, and supporting, and defending organizational objectives.

Williams and Anderson (1991) conceptualized a framework that focused on the target rather than the context of behavior. This framework defined OCBI as those helpful behaviors directed toward other individuals (e.g. helping others who have been absent) and OCBO as those behaviors that benefit the organization (e.g. attendance at work is above the norm). While meta-analysis has brought into question whether the distinction between facets of OCB is meaningful (LePine, Erez, & Johnson, 2002), they are measured separately for this thesis, because of the conceptual relationships with cyber-security behaviors.

OCBs and Cyber Behaviors

To the best of my knowledge, past research has not yet investigated the relationship between OCBs and cyber-security behaviors. Thus, the third goal of this thesis is to determine if cyber behaviors and OCBs are related. By understanding the relationship between citizenship behaviors and cyber behaviors, researchers can gain a better understanding about the nature and measurement cyber behaviors. Security assurance behaviors are those behaviors taken by an employee that actively protect an organization's information (Guo, 2013). Because these behaviors involve a proactive component to help the organization, they are conceptually related to organizationally directed OCBs. Similarly, security compliance behaviors will be related to organizationally directed OCBs. While security compliance behaviors do not necessarily involve behaviors that proactively protect the organization's information, cyber-security compliance is not typically considered part of an employee's task performance and may be viewed by the employee as an action that goes above and beyond their expected job performance. See Figure 1 for the conceptual model. Thus, I hypothesize the following relationships:

Hypothesis 5a: Organizationally directed organizational citizenship behaviors will be positively related to security assurance behaviors.

Hypothesis 5b: Organizationally directed organizational citizenship behaviors will be positively related to security compliance behaviors.

Hypothesis 5c: Security assurance and security compliance behaviors will be more strongly related to organizationally directed citizenship behaviors than interpersonally directed citizenship behaviors.

Counterproductive Work Behaviors

Counterproductive work behaviors (CWBs) are often defined as employee behaviors that are viewed as contrary to the goals of the organization (Sackett & Devore, 2001). Additionally, these behaviors have the possibility, but not guarantee of causing harm to the organization, which is important because it reflects nature of the behaviors themselves, not outcomes (Hoffman & Dilchert, 2012). While some authors define CWBs as intentional behaviors (Robinson & Bennett, 1995; Sackett, 2002), others view this idea as problematic, because some unintentional employee behaviors are contrary to the legitimate interests of the organization (Hoffman & Dilchert, 2012; Motowidlo, 2003). Though there has been some debate about the underlying structure of CWBs, Robinson and Bennett's (1995) conceptual model of CWBs is widely used in the literature. Using multidimensional scaling, Robinson and Bennett (1995) identified four quadrants of deviant behaviors along two dimensions, severity and target of those deviant behaviors. The first quadrant, labeled property deviance, involves serious, organizationally directed deviant behaviors. The second quadrant, labeled property deviance, involves minor, organizationally directed deviant behaviors. The third quadrant, political deviance, involves interpersonally directed but minor deviant behaviors. The last quadrant, personal aggression, involved severe, interpersonally directed behaviors.

Using this work as a basis for scale development, Bennett and Robinson (2000) developed and validated a workplace deviance scale with two subscales, organizational deviance (OD) and interpersonal deviance (ID). Organizational deviance is defined as behaviors, which employees engage that are targeted towards the organization (e.g. damaging company property, sharing confidential company information), while interpersonal deviance is defined as those behaviors in which employees perform that are targeted towards other individuals (e.g. gossip,

theft from coworkers) (Bennett and Robinson, 2000; Berry, Ones, & Sackett, 2007). Confirmatory factor analysis offered support for this two-factor model, and there is evidence for both convergent and discriminant validity (Bennett & Robinson, 2000). While there has been some criticisms that the high correlation ($\rho = .62$) between these two factors indicates that they are empirically indistinguishable, Berry, et al. (2007) meta-analytically determined that the differential relationships between the two factors and the Big Five and OCBs indicated that these factors are separate.

CWBs and Cyber Behaviors

Similar to OCBs, no past research has examined the relationships between cyber related behaviors and CWBs. Therefore, one of the goals of this thesis is to determine if cyber behaviors are similar to certain forms of CWBs. Conceptually, there are several reasons while security risk and damaging behaviors will be related to organizational deviance (See Figure 2 for the conceptual model). First, both risk and damaging behaviors involve those behaviors that have the potential of harming the organization (Guo, 2013). Second, these behaviors can be intentional or unintentional, much like traditional definitions of CWBs. Third, security risk and damaging behaviors are organizationally, rather than interpersonally directed, because they put an organization's information security at risk, rather than directly harming specific individuals (Guo, 2013). Thus I propose the following hypotheses:

Hypothesis 6a: Organizationally directed counterproductive work behaviors will be positively related to security risk behaviors.

Hypothesis 6b: Organizationally directed counterproductive work behaviors will be positively related to security damaging behaviors.

Hypothesis 6c: Security risk and security damaging behaviors will be more strongly related to organizational deviance than interpersonal deviance.

Chapter Two
Method

Participants and Procedure

Participants were 477 individuals recruited through Amazon Mechanical Turk system who work in the United States at a variety of organizations and occupations. Participants were required to work at least 10 hours per week, work in the United States, and use a computer at work. The sample was 52.6% female and an average age of 36 years old (*SD* = 11.86). Participants reported working an average of 38.37 hours (*SD* = 10.13) per week and using a computer an average of 26 hours (*SD* = 14.35) per week while at work. Additionally, 6.5% of participants working in an information technology related job (e.g. systems administrator, programmer). 42.8% of participants held a bachelor's degree, 23.5% had some college, 10.9% held an associate's degree, 9.9% a master's degree, and 2.7% a professional or doctoral degree.

Participants who were interested in completing the study posted on Amazon Turk's website received a link to an external Qualtrics survey. They were first asked to read and acknowledge an understanding of the consent form, giving consent to participate in the study. Next, they completed several demographic questions (e.g. gender, age, job title), frequency of computer use at work, a measure of perceptions of penalty severity, the IPIP personality self-report inventory, the OCB and CWB measures, and the cyber-security behavior inventory. To ensure confidentiality, no participant names or personal information were attached to the responses. Due to the sensitive nature of the questions and to ensure the most honest responses,

participants were assured that this information would be used for research purposes only. Participants were compensated $.50 for completing the survey.

Measures

Cyber-Security Behaviors

Cyber-security behaviors were measured using a 23-item scale comprised of self-developed and items adapted from previous research, based on Guo's (2013) conceptual model. These items measured a wide range of cyber-security behaviors that may be useful in understanding the underlying factor structure of cyber-security behaviors. Participants were asked to respond to the statement "Please indicate the frequency in which these you have engaged in each of the following behaviors in the past year" on a 7-point Likert scale, ranging from 1 (never) to 7 (16 or more times). See Appendix A for the complete list of items.

Big Five Personality

The Big Five personality factors were measured using the 10-item International Personality Item Pool (IPIP) (Goldberg, 1999; Goldberg et al., 2006) scales for emotional stability, extraversion, openness to experience, agreeableness, and conscientiousness. The scale will contain a total of 50 items. The scales showed good internal consistency in the current study, with $\alpha = 0.79$ for emotional stability, $\alpha = 0.89$ for extraversion, $\alpha = 0.84$ for openness to experience, $\alpha = 0.87$ for agreeableness, and $\alpha = 0.84$ for conscientiousness.

Organizational Citizenship Behaviors

Organizational citizenship behaviors were adapted from Williams and Anderson's (1991) measures of OCBI (7 items) and OCBO (6 items). Both the OCBI and OCBO scales had adequate reliability ($\alpha = .78$ and .69, respectively). Participants were asked to respond to the statement "Please indicate the frequency in which these you have engaged in each of the

following behaviors in the past year" on a 5-point Likert scale, ranging from 1 (never) to 5 (always).

Counterproductive Work Behaviors

Counterproductive work behaviors were measured using Bennett and Robinson's (2000) scales measuring interpersonal and organizational deviance. The 7-item interpersonal deviance scale showed excellent reliability ($\alpha = .91$), as did the 12-item organizational deviance scale ($\alpha = .90$). Participants were asked to indicate the frequency, which they have engaged in each behavior in the past year on a 5-point Likert scale, ranging from 1 (never) to 5(always).

Demographics and Control Variables

In addition to the above measures, participants were asked to report their age, gender, level of education, weekly computer use at work, job tenure, job title, and perceived severity of punishment. Perceptions of severity of penalty for breaking organizational security rules were measured using 3 items adapted from Herath and Rao (2009). This scale included the questions "The organization disciplines employees who break information security rules", "My organization terminates employees who repeatedly break security rules", and "If I were caught violating organization information security policies, I would be severely punished" (Herath and Rao, 2009, p. 164), and were measured on a 7-point Likert scale (Strongly Disagree to Strongly Agree). The scale had good reliability ($\alpha = .88$). Because perceptions of severity of penalty could affect the frequency of cyber-security behaviors, this data was analyzed with this construct as a control.

Chapter Three
Results

Frequency of Cyber-Security Behaviors

Means, standard deviations, range, and frequency of all cyber-security scale items are presented in Table 3. Because participants reported the frequency in which they performed a variety of cyber-security related behaviors, it is interesting to evaluate the extent to which employees from a wide variety of occupations are performing not only positive, but also negative cyber behaviors. An overwhelming majority of respondents reported using a secure password (i.e. a password containing letters, numbers, and symbols) for their work computer (93.1%), following information security policies (95.6%) and using good information security practices at work, though less than half (43.8%) reported that they change their password more often than their employer requires. Most respondents also reported that they monitor their work computer for signs of a virus or malware (75.3%) and immediately delete suspicious emails on their work email without reading them (79.5%). 75.3% of respondents said they have walked away from their computer without locking it first, while about a quarter reported that they have shared their work account user name or password with a friend or coworker (24.3%) or written their password down and left it where others might see it (28.1%). 35.1% of respondents reported that they have copied work information onto a personal USB drive, 21.2% have communicated confidential information on an unsecured network, and 12.6% have tried to crack the firework on their work computer to access prohibited websites. While it is evident that positive cyber

behaviors are more prevalent, it is important to note that a substantial proportion of respondents have engaged in risky or potentially damaging cyber behaviors in the past year.

Cyber-Security Scale Dimensions

In order to answer research question 1, factor analysis was used evaluate the dimensions of cyber security behaviors using a 23-item scale. Because no prior research has looked at a full range of behaviors within one scale, exploratory factor analysis was used to first determine the most likely factor structure, followed by confirmatory factor analysis to validate the results from the EFA. In order to conduct the EFA, I randomly selected approximately half of the responses from the overall sample, resulting in a sample of 238 participants. EFA operates under the common factor model, which assumes that each measured variable had common and unique variance, and that underlying common factors can explain the correlations among measured variables.

Two commonly used extraction algorithm for EFA are maximum likelihood (ML) and principal axis factoring (PAF). Each method estimates parameters according to assumptions of the common factor model, but differ in how those parameters are estimated (Fabrigar & Wegener, 2012). Both ML and PAF are iterative techniques, meaning that they repeat until the communalities between two different iterations are very similar, however solutions need to be rotated for interpretability (Fabrigar & Wegener, 2012). ML assumes that the data are based on a random sample and that the measured variables have a multivariate normal distribution (Fabrigar & Wegener, 2012). The goal of ML is to estimate the factor loadings and unique variances as to maximize the likelihood function. Unlike PAF, ML provides a likelihood ratio test (χ^2) statistic as an indicator of model fit, though it is highly sensitive to sample size. While ML provides additional information about fit and performs slightly better than PAF when factors are

correlated and there are unequal loadings within factors (de Winter & Dodou, 2012), it tends to over factor solutions. Additionally, PAF is typically good at recovering factors with low loadings (de Winter & Dodou, 2012).

While in general both ML and PAF are reasonable extraction techniques for EFA, PAF provides a more robust solution in circumstances where the observed variables are non-normal (Fabrigar et al., 1999). Evaluation of items on the cyber-security scale indicated that some items intended to measure security damaging behaviors were significantly positively skewed, and had significant kurtosis. The non-normality of these types of behaviors is not unexpected however, given the infrequency of some of the more extreme cyber damaging behaviors. Because of the moderate violation of non-normality, ML is inappropriate to use as an extraction technique. Therefore PAF was used as the factor identification and extraction technique for EFA.

Because the factors of cyber-security behaviors are likely correlated, oblique rotation was used in the analysis. One of the most commonly used oblique rotation methods is promax rotation, which transforms the initial solution by raising factor loadings to a power of two or more (Fabrigar & Wegener, 2012). Factor loadings are raised by the kappa parameter, and higher values produce bigger correlations between factors (Fabrigar & Wegener, 2012). Given the sufficiency of results produced by promax, this rotation method was used.

The initial factor analysis with promax with Kaiser Normalization extracted five factors that were shown on the scree plot, and had an eigenvalue greater than one. Items with factor loadings lower than .4 were used as a cutoff. Though a fifth factor was extracted during the factor analysis, no items loaded strongly onto this factor. Therefore, in order to extract a more parsimonious solution, the EFA was rerun with a maximum of 4 factors extracted. This four factor solution converged after 7 iterations and items with factor loadings lower than .4 were

deleted. Items “Immediately deleted suspicious emails in your work email without reading them” and “Refused to tell anyone your work ID or password” were heavily cross loaded on factors 2 and 4, and were subsequently deleted from the scale. The factor analysis was rerun on the remaining 21 items to obtain a final 4-factor solution, which is readily interpretable. In this solution, each item loaded strongly onto one factor. Together, the four factors accounted for 57.8% of the variance. Item factor loadings and factors are presented in Table 4. For the purposes of this paper and to be consistent with proposed hypotheses, the final four factors extracted were labeled security assurance behaviors (SABs), security compliance behaviors (SCBs), security risk behaviors (SRBs), and security damaging behaviors (SDBs).

Security damaging behaviors accounted for the most variance (31.4%) and therefore appeared to be most important for the scale, perhaps in part because this dimension contained the most items. This dimension is comprised of items SDB 1-6, as well as SRB4, SRB5, and SRB6. This dimension seems to encompass not only some of the more severe behaviors, but also some risk behaviors such as copying work information on a personal USB drive, installing unauthorized software from the internet onto your computer, and using your social security number as your password. The security compliance behaviors dimension accounted for second most variance (13.1%), and is comprised of items SCB 1-4, as well as SAB4 (using a secure password for your work computer). While SAB4 was originally intended to measure an assurance behavior, it is not unreasonable for this to be considered a security compliance behavior, given that many companies require employees to use strong passwords for their user accounts. The third dimension, security risk behaviors, accounted for 7.78% of the variance, and was comprised of SRB1, SRB2, SRB3, and SRB7. These items all involved behaviors about computer passwords, so it makes theoretical sense that these items loaded together. The last

dimension, security assurance behaviors, accounted for 5.61% of the variance and is comprised of items SAB1, SAB5, and SAB6, which measured the frequency in which people monitor their work computer for signs of a virus/malware, changed their password frequency, or went above and beyond what their organization required to protect their work information.

Scale Validation

In order to validate the factor structure of the cyber-security scale, confirmatory factor analysis was conducted on the second half of the data (N = 239) not used in the exploratory factor analysis. As with EFA, one of the most common estimation methods is maximum likelihood, which assumes normality in the data. Because there is evidence of non-normality in the data, I used an alternative estimation method, MLR, which has standard errors robust to non-normality and an adjusted chi-square statistic that uses a scaling factor to correct for the degree of non-normality (Satorra & Bentler, 1994). A four-factor model based on the results of the exploratory factor analysis was fit to the data using Mplus. A marker variable strategy, in which the first item on each latent factor is fixed to 1.00, was used for model identification purposes.

In order to determine if the model fit the data, overall fit indices, factor loadings, and residual correlations were considered. When examining overall fit indices, a non-significant chi-square test indicates any differences between the observed and model-implied covariance matrices may be due to sampling error and it can be argued that the model is plausible. Standardized root mean squared residual (SRMR), root mean square error of approximation (RMSEA), comparative fit index (CFI), and Tucker-Lewis (TLI) were evaluated for overall fit. According to the recommendations of Hu and Bentler (1999), smaller SRMR values indicate better fit and values less than .08 indicate adequate fit and RMSEA values less than .06 are

considered good fit. CFI and TLI both index the discrepancy between the tested model and null model, and values greater than .95 indicate good fit.

For this model, the Satorra-Bentler chi-square test was significant (χ^2 = 346.815, p <.001) however this fit measure is highly sensitive to sample size and other fit indices should be considered. CFI and TLI were .86 and .84 respectively, which indicated adequate fit. RMSEA was .06 and SRMR was .07, also indicating good fit. Additionally, standardized factor loadings were adequate (most over .6) with the exception of one item, "walked away from your computer without locking it first", which had a non-significant loading (.177) on the SRB factor. Because the model did not explain significant variance in that item and in consideration of parsimony in the scale, the item was removed and the subsequent factor model was fit to the data. Removal of that item resulted in an improvement in global model fit indices. While the Satorra-Bentler chi-square test statistic was still significant (χ^2 = 290.99, p <.001), other measures of fit improved (CFI = .89, TLI = .87, RMSEA=.057), standardized factor loadings ranged from .40-.89 (See Table 5). Because the models were non-nested, I could not conduct a scaled chi-square difference test, however with the consideration of theory and parsimony in the scale, the model without SRB7 is preferred in this case. See Table 6 for global fit indices of both models.

In order to compute scale reliability for each cyber-security subscale, I used composite reliability rather than Cronbach's alpha. Because loading values are unequal within each scale, composite reliability is preferred over alpha because alpha tends to underestimate reliability (Raykov, 1997). The reliabilities were .63, .75, .63, and .89 for SAB, SCB, SRB, and SDB dimensions, respectively. The low reliability for the SAB and SRB scales may be due to the heterogeneity and low number of items in each scale. Interfactor correlations suggested that the factors are related, but unique. The SAB dimension is significantly related to SCB and SDB (.44

and .13, respectively), but not to SRB (.043, p = .62). SCB was significantly negatively related to SRB (-.35, p<.01) and SDB (-.33, p<.01). SRB and SDB were significant positively related (.75, p<.001). Thus, for the purposes of hypothesis testing, the final cyber-security scales contained 3, 5, 3, and 9 items measuring SABs, SCBs, SRBs, and SDBs, respectively.

Hypothesis Testing

For all further analyses, the entire sample was used (N = 477). Means, standard deviations, skewness, and kurtosis values for all study variables are presented in Table 7. As previously discussed, cyber-security behaviors, organizational citizenship and counterproductive work behaviors were measured on 7 and 5-point Likert scales, respectively, with "1" indicating that respondents had not performed that behavior in the past year. Personality was measured on a 5-point Likert scale of accuracy, with "3" indicating that a given personality item was neither inaccurate nor accurate in describing the respondent. Overall, respondents performed more individually directed (*M* = 3.65, *SD* = .67) and organizationally directed (*M* = 4.08, *SD* = .58) organizational citizenship behaviors (OCBs) than individually directed (*M* = 1.47, *SD* = .66) and organizationally directed (*M* = 1.64, *SD* = .61) counterproductive work behaviors (CWBs). Similarly, they performed more SABs (*M* = 3.48, *SD* = 1.50) and SCBs (*M* = 5.48, *SD* = 1.39) than SRBs (*M* = 1.95, *SD* = 1.18) and SDBs (*M* = 1.46, *SD* = .81).

Next, correlational analyses were conducted to test select hypotheses. See Table 8 for zero-order correlations between all variables. Reliabilities are reported on the diagonal, and are coefficient alpha for all scales, except for the cyber-security dimensions, which are composite reliability. Security assurance behaviors were positively related to conscientiousness (*r* = .18, *p* <.001), agreeableness (*r* = .15, *p* <.001), openness to experience (*r* = .11, *p* <.05), supporting Hypotheses 1a, 1c, and 1e. Though not hypothesized, emotional stability was also positively

related to SABs (r = .19, p <.001). It should be noted that due to the low reliability of this scale, however, relationships could be attenuated. Conscientiousness was positively related to security compliance behaviors (r = .27, p <.001), supporting Hypothesis 2a. Additionally, agreeableness (r = .29, p <.001), openness to experience (r = .27, p <.001), and emotional stability (r = .21, p <.001) were positively related to SCBs. Conscientiousness was negatively related to security risk behaviors (r = -.21, p <.001), supporting hypothesis 3a. Agreeableness (r = -.14, p <.01), openness to experience (r = -.16, p <.001), and emotional stability (r = -.18, p <.001) were also negatively related to SRBs. Lastly, conscientiousness (r = -.32, p <.001), agreeableness (r = -.29, p <.001), and emotional stability (r = -.11, p <.05), were negatively related to security damaging behaviors supporting hypotheses 4a, 4c, and 4e.

Additional correlational analyses were conducted to determine if cyber-security behaviors were related to two types of organizational citizenship and counterproductive work behaviors. SABs were significantly, positively related to both individually directed (r = .18, p <.001) and organizationally directed (r = .15, p <.01) OCBs, which supports hypothesis 5a. Additionally, SCBs were significantly, positively related to both individually directed (r = .22, p <.001) and organizationally directed (r = .44, p <.001) OCBs, which supporting hypothesis 5b. Conversely, organizationally directed OCBs are strongly, negatively related both SRBs (r = -.40, p <.001) and SDBs (r = -.55, p <.001). Therefore, it appears that individuals who are engaging in beneficial behaviors towards their organization are complying with or going above and beyond organizational policy but are engaging in fewer risky or damaging cyber behaviors. SRBs were significantly positively related to interpersonal deviance (r = .43, p <.001) and organizational deviance (r = .48, p <.001), supporting hypothesis 6a. SDBs were also significantly positively related to interpersonal deviance (r = .61, p <.001) and organizational deviance (r = .61, p

<.001), supporting hypothesis 6b. These results suggest that individuals who are engaging in counterproductive work behaviors are also engaging in cyber-security risk and damaging behaviors.

Post hoc t-tests were conducted with Steiger's (1980) equation for dependent correlations to test hypotheses 5c and 6c and examine if the correlations previously mentioned are significantly different from each other. Hypothesis 5c stated that SABs and SCBs would be more strongly related to OCBs than interpersonally directed OCBs. Post hoc analysis revealed that the correlation between SABs and individually directed OCBs is not significantly different from the correlation between SABs and organizationally directed OCBs (t = .65, p =.52). However, the correlation between SCBs and organizationally directed OCBs was significantly higher than the correlation between SCBs and individually directed OCBs (t = -4.68, p <.001).Thus, hypothesis 5c was partially supported. Hypothesis 6c stated that SRBs and SDBs would be more strongly related to organizational deviance than interpersonal deviance. There were no significant differences in the relationships between SRBs and both types of deviance (t = -1.81, p =.07). Similarly, there were no significant differences between SDBs and both types of deviance (t = .14, p =.89). Therefore, hypothesis 6c was not supported.

A series of hierarchical linear regressions analyses were performed to test the remaining hypotheses. Upon further examination of the correlation table, it is important to note that age, gender, frequency of computer use, and severity of punishment were significantly related to at least one type of cyber behavior. Therefore, those variables were entered into the subsequent regression equations in step 1 as controls. See Tables 9-12 for individual regression results. In order to test hypothesis 1b, conscientiousness was entered into the regression equation in step 2 for predicting SABs. Regression results indicated that conscientiousness was predictive of SABs

(β =.15, p <.01), even when controlling for demographics and severity of punishment, which was also a significant predictor (β =.18, p <.001). Thus, hypothesis 1b was supported. Agreeableness (β =.14, p <.01) and Openness to Experience (β =.10, p <.05) were also significantly, positively predictive of SABs, supporting hypotheses 1d and 1f. These results suggest that individuals with higher levels of conscientiousness, agreeableness, or openness to experience may be more likely to engage in cyber assurance behaviors. Conscientiousness was a significant predictor of SCBs (β =.19, p <.001), meaning that higher levels of conscientiousness are predictive of more compliant behavior. This supports hypothesis 2b. Additionally, older individuals (β =.17, p <.001), those who spend more time on the computer (β =.13, p <.01) and those who perceive that they will be punished for breaking information security rules (β =.15, p <.01) are also more likely to engage in compliant behavior.

Conscientiousness was significantly, negatively predictive of SRBs (β =-.18, p <.001), suggesting that individuals lower in conscientiousness are more likely to engage in risky cyber behavior (hypothesis 3b – supported). Additionally, those who perceive higher severity of punishment are less likely to engage in these behaviors (β =-.10, p <.01). Lastly, conscientiousness (β =-.25, p <.001) and agreeableness (β =-.19, p <.001) were both individually predictive of SDBs, such that individuals lower on these traits were more likely to engage in damaging behaviors. These results support hypotheses 4b and 4d. Emotional stability, however, was not a significant predictor of SDBs (β =-.08, p =.09), so hypothesis 4f was not supported. Additionally, younger (β =.18, p <.001), male (β =.18, p <.001) participants were more likely to engage in SDBs at work.

Additional Analyses

Additional hierarchical regression analyses were conducted to determine if hypothesized personality traits were incrementally predictive of cyber-security behaviors beyond other Big Five traits. Results showed that conscientiousness, agreeableness, and openness to experience did not predict SABs above and beyond other Big Five traits. Similarly conscientiousness was not significantly incrementally predictive of SCBs or SRBs over the other four Big Five traits. However, conscientiousness had significant incremental validity in predicting SDBs over the other Big Five traits (β =-.20, p <.001), as did agreeableness (β =-.13, p <.05). This indicates that these personality traits may be especially helpful in predicting individuals who will engage in more severe cyber-security behaviors.

Chapter Four
Discussion

The first goal and research question of this thesis was to explore the dimensionality of Guo's (2013) recent conceptualization of cyber-security behaviors. Using the existing literature, a scale was constructed using items measuring each dimension of this framework. The scale consisted of a wide variety of cyber-security related behaviors, ranging from positive, proactive behaviors (e.g. checking your computer for signs of a virus) to more malicious behaviors (e.g. cracking the firewall on a company computer). Respondents reported engaging in positive and compliant behaviors more often than risky and damaging, which is good news for organizations. However, the fact that employees are engaging negative behaviors should be of concern to organizations, because even one occurrence of a risky cyber related behavior by an employee can lead to damaging consequences for an organization (Crossler et al., 2013). For example, 28.1% of participants reported that they had written down their work password where others might see it. While this behavior itself does not cause immediate damage to an organization's information, someone with malicious intent could see that password and use it to gain unauthorized access to that information.

Factor analysis revealed that there are four factors underlying the items of the new cyber-security scale, which is consistent with the framework suggested by Guo (2013). These factors are labeled security assurance behaviors, security compliance behaviors, security risk behaviors, and security damaging behaviors. Most items load onto their respective factors, with the exception of the security damaging behaviors dimension. Because some items that were

originally intended to measure a "risk" behavior, not "damaging" behavior, load on the same factor as some of the more extreme behaviors, there could be some other underlying commonality about the behaviors beyond the properties suggested by Guo (2013). Given that all of the items in this dimension seem to get at behaviors that are counterproductive to an organization's information security, that dimension might be best labeled as "counterproductive cyber behavior" for use in future research.

Correlation and regression analyses reveals that several Big Five personality traits are significantly related to, and predictive of, cyber-security behaviors. Conscientiousness, agreeableness, and openness to experience are all significantly positively correlated with and predictive of security assurance behaviors. This means that individuals higher on these traits are more likely to go above and beyond what is expected to protect their organization's information security. These findings are consistent with Chiaburu et al. (2011), who found that these three traits are the strongest predictors of prosocial behavior at work. Additionally, individuals high in openness might be more receptive to any information security training they may have received, which often encourages employees to proactively protect their work information.

Consistent with past research on cyber-security rule following behavior (Hu et al., 2012), conscientiousness is significant related to, and predictive of, security compliance behaviors. Individuals high in conscientiousness are aware of and may want to follow the rules of their organization; therefore, they adhere to the information security policies put in place by their organization. Additionally, agreeableness, openness to experience, and emotional stability are positively related to complaint behavior. Similar to security assurance behaviors, those high in agreeableness and openness may be more receptive for security training, while those high in emotional stability have more self-discipline and therefore may be more likely to follow

compliant procedures rather than risky behavior. Additionally, an interesting, but perhaps not surprising finding is that individuals who perceive that they will be punished for breaking the rules are more likely to engage in compliant behavior. Theoretically, if an individual feels like they will get in trouble for breaking the rules, they will be less likely to break those rules.

Conscientiousness is significantly negatively related to, and predictive of, security risk behaviors, a dimension that is comprised of items specifically involving risky password behaviors. Individuals who are lower in conscientiousness might not consider the consequences of actions such as leaving a password where others might see it or sharing that information with coworkers or friends. Agreeableness, openness to experience, and emotional stability are also negatively related to risk behaviors. These findings contradict those by Whitty, Doodson, Creese, and Hodges (2015), who found that individuals higher on openness to experience were more likely to share their password with others. Individuals who perceived a higher severity of punishment are less likely to engage in risky behaviors, possibly because the consequences were too high if they were to get caught.

As hypothesized, conscientiousness, agreeableness, and emotional stability are negatively related to security damaging behaviors. While regression analyses reveals that conscientiousness and agreeableness are predictive of security damaging behaviors, emotional stability did not predict these behaviors when controlling for age, sex, computer use, and severity of punishment. This finding is consistent with Berry et al., (2007) who found that these traits are related to deviant behavior. Individuals low in conscientiousness and agreeableness may not take consequences of their actions in to consideration, or may even maliciously act against their organization if it is beneficial to them. Consistent with prior literature (Whitty et al., 2015), younger individuals were more likely to engage in security damaging behaviors, perhaps because

they are more comfortable with technology than older individuals and possess the knowledge to engage in the behaviors measured by this dimension that require more technological expertise.

Positive cyber behaviors (security assurance and compliance behaviors) are both positively related to individually directed and interpersonally directed organizational citizenship behaviors. Employees who go above and beyond their task performance are also likely to engage in proactive and compliant cyber behaviors, because they likely have a desire to help their organization. Even though compliant cyber behaviors do not necessarily have a proactive component from an information security perspective, employees may view them as going above and beyond what is required of them because cyber related behaviors are often not considered an inherent part of their task performance. Follow-up analyses indicated that security compliance behaviors are more strongly related to organizationally-directed organizational citizenship behaviors than individually directed organizational citizenship behaviors, possibly because complying with organizational cyber policy is a similar behavior to engaging in other behaviors that help the organization, rather than coworkers.

Results also indicated that security risk behaviors and security damaging behaviors are strongly, positively related to both interpersonal and organizational deviance. Given that organizational citizenship behaviors are positively related to positive cyber behaviors, it makes sense that counterproductive work behaviors are related to negative cyber behaviors. Individuals who engage in undesirable behaviors toward their coworkers and organization are also engaging in behaviors that could put their organization's information at risk. Additionally, security risk behaviors and security damaging behaviors are strongly, negatively related to organizationally directed organizational citizenship behaviors. Overall, these findings indicate that individuals

who are engaging in behaviors to help their organizational are not necessary the same individuals who are engaging in risky or damaging cyber behaviors.

Implications

Overall, there are a number of interesting findings of this study. First, cyber behaviors can potentially be grouped in four distinct dimensions. Second, that while a perhaps more distal than constructs such as organizational norms or attitudes, personality traits are related to and predict cyber behaviors. This suggests that organizations may be able to use traditional personality screening and selection measures to identify employees who may be more likely to engage in cyber behaviors of interest. Managers should be mindful of the heterogeneity of personalities of their employees and tailor cyber training programs and workshops accordingly. Selection, in addition to training for cyber awareness, can also potentially reduce the frequency of cyber risk behaviors by employees. Third, the finding that OCBs relate positively to SABs and SCBs, and negatively to SRBs and SDBs suggest that same types of people who are helping the organization are also not harming it. Therefore, by hiring and retaining employees who are frequently engaging in OCBs and other positive behaviors, an organization may be able to more easily foster a culture where positive cyber behaviors are also the norm.

Given the finding that perceptions of severity of punishment were predictive of reduced SRBs and SDBs, organizations should make it clear to employees that risky and damaging behaviors will not be tolerated and that consequences are just as severe as breaking other organizational rules. Additionally, companies should make their policies transparent to employees, so that there is little ambiguity about what constitutes a negative cyber behavior. These practices, along with careful selection of employees, can potentially help reduce the risk of insider threat.

Limitations and Suggestions for Future Research

While this research contributes to the rapidly growing body of cyber-security literature, it has several limitations. First, the reliability of the SAB and SRB factors is low, which may have attenuated the relationships between these dimensions and other study variables. Further, the behaviors in this scale were not inclusive of all cyber-related behavior, but rather a sampling of behaviors, especially given that technology keeps evolving. New threats mean new opportunities for information leaks in organizations, and the opportunities for employees to engage in risky or damaging behaviors only grow. Future research could consider additional threats such as phishing scams to identify other ways that employees might potentially put organizational information security at risk.

Because of the cross sectional nature of this study, it is difficult to prove that personality is causing employees to engage in certain behaviors. Though it is unlikely that cyber behaviors shape an employee's personality, it is impossible to say with certainty that there is no bidirectional relationship. Additionally, because all measures were self-report, participants could have been inaccurate or misleading about how frequently they engaged in various behaviors. For example, an employee reporting that they frequently engage in positive cyber behaviors might believe they are complying with information security policy, but by company standards they are not. Lastly, this study did not capture the opportunity to perform each behavior. Two employees within different organizations may both have similar intentions to engage in a risky behavior, but only one might actually perform that behavior if the opportunity arises. It may be fruitful for future research to investigate role of opportunity in the link between intention and behavior.

Given these findings, future research should also investigate the interaction between personality and situation within a given organization, and its influence on employee cyber

behaviors. Combining these distal and more proximal factors may give a more complete picture of why employees engage in these behaviors. For example, individuals low in conscientiousness may be more likely to engage in risky behavior only when there are ambiguous rules surrounding that behavior, whereas those high in conscientiousness might be less likely to break the rules regardless of rule ambiguity.

Conclusion

The current study sought to investigate the previously understudied relationships between cyber-security behaviors, personality, and organizational and counterproductive work behaviors. Unlike past research, it evaluated the prevalence and antecedents of actual cyber-security behaviors, rather than attitudes or intentions. Results demonstrate that cyber-security related behavior can be separated into four distinct categories and that personality traits such as conscientiousness, agreeableness, and openness to experience are predictive of the spectrum of cyber behavior. Further, cyber-related behaviors are related organizational and counterproductive work behaviors. This research suggests that personality is a useful predictor for cyber-security behaviors and can potentially be used to mitigate insider threat in the workplace.

References

Barrick, M. R., & Mount, M. K. (1991). The big five personality dimensions and job performance: a meta-analysis. *Personnel psychology*, *44*(1), 1-26.

Becton, J. B., Matthews, M. C., Hartley, D. L., & Whitaker, L. D. (2012). Using biodata as a predictor of errors, tardiness, policy violations, overall job performance, and turnover among nurses. *Journal of Management & Organization*, *18*(5), 714-727.

Bennett, R. J., & Robinson, S. L. (2000). Development of a measure of workplace deviance. *Journal of Applied Psychology*, *85*(3), 349.

Berry, C. M., Ones, D. S., & Sackett, P. R. (2007). Interpersonal deviance, organizational deviance, and their common correlates: A review and meta-analysis. *Journal of Applied Psychology*, *92*(2), 410-424. doi:10.1037/0021-9010.92.2.410

Borman, W. C., & Motowidlo, S. M. (1993). Expanding the criterion domain to include elements of contextual performance. Chapter in N. Schmitt and W. C. Borman (Eds.), Personnel selection in organizations (pp. 71-98). San Francisco: Jossey-Bass.

Chiaburu, D. S., Oh, I., Berry, C. M., Li, N., & Gardner, R. G. (2011). The five-factor model of personality traits and organizational citizenship behaviors: A meta-analysis. *Journal of Applied Psychology*, *96*(6), 1140-1166. doi:10.1037/a0024004.

Costa, P. T., & McCrae, R. R. (2008). The Revised NEO Personality Inventory (NEO-PI-R). *The SAGE handbook of personality theory and assessment*, *2*, 179-198.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2012). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.

de Winter, J. C. F., & Dodou, D. (2012). Factor recovery by principal axis factoring and maximum likelihood factor analysis as a function of factor pattern and sample size. *Journal of Applied Statistics*, *39*(4), 695-710.

de Winter, J. C. F., Dodou, D., & Wieringa, P. A. (2009). Exploratory factor analysis with small sample sizes. *Multivariate Behavioral Research*, *44*(2), 147-181.

DeYoung, C. G. (2006). Higher-order factors of the Big Five in a multi-informant sample. *Journal of Personality and Social Psychology*, *91*, 1138– 1151.

DeYoung, C. G., Quilty, L. C., & Peterson, J. B. (2007). Between facets and domains: 10 aspects of the Big Five. *Journal of Personality and Social Psychology*, *93*(5), 880-896.

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological methods*, *4*(3), 272.

Fabrigar, L. R., & Wegener, D. T. (2012). *Exploratory Factor Analysis*. New York, New York: Oxford University Press.

Fiske, D. W. (1949). Consistency of the factorial structures of personality ratings from different sources. *The Journal of Abnormal and Social Psychology, 44*(3), 329-344.

Goldberg, L. R. (1999). A broad-bandwidth, public domain, personality inventory measuring the lower-level facets of several five-factor models. In I. Mervielde, I. Deary, F. De Fruyt, &

F. Ostendorf (Eds.), *Personality Psychology in Europe*, Vol. 7 (pp. 7-28). Tilburg, The Netherlands: Tilburg University Press.
Goldberg, L. R., Johnson, J. A., Eber, H. W., Hogan, R., Ashton, M. C., Cloninger, C. R., & Gough, H. C. (2006). The International Personality Item Pool and the future of public-domain personality measures. *Journal of Research in Personality, 40*, 84-96.
Guo, K. H. (2013). Security related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242-251.
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.
Hendrickson, A. E., & White, P. O. (1964). Promax: A quick method for rotation to oblique simple structure. *British Journal of Statistical Psychology*, *17*(1), 65-70.
Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.
Hoffman, B. J., & Dilchert, S. (2012). A review of citizenship and counterproductive behaviors in organizational decision-making. *The Oxford Handbook of Personnel Selection and Selection*, 543-569.
Hollenbeck, J. R., & Whitener, E. M. (1988). Reclaiming personality traits for personnel selection: Self-esteem as an illustrative case. *Journal of Management*, *14*(1), 81-91.
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), 615-659.
Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *ACM SIGMIS Database*, *36*(4), 68-79.
International Personality Item Pool: A Scientific Collaboratory for the Development of Advanced Measures of Personality Traits and Other Individual Differences (http://ipip.ori.org/). Internet Web Site.
Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, *48*(4), 15-24.
Lazar, J., Jones, A., Hackley, M., & Shneiderman, B. (2006). Severity and impact of computer user frustration: A comparison of student and workplace users. *Interacting with Computers*, *18*(2), 187-207.
LePine, J. A., Erez, A., & Johnson, D. E. (2002). The nature and dimensionality of organizational citizenship behavior: a critical review and meta-analysis. *Journal of Applied Psychology*, *87*(1), 52-65.
Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, 173-186.
Mael, F. A. (1991). A conceptual rationale for the domain and attributes of biodata items. *Personnel Psychology*, *44*(4), 763-792.
McCrae, R. R., & Costa, P. T, Jr. (1985). Updating Norman's "adequate taxonomy": Intelligence and personality dimensions in natural language and in questionnaires *Journal of Personality and Social Psychology, 49*, 710-721.
McCrae R.R., Costa P.T. Jr. (1987). Validation of the five-factor model of personality across instruments and observers. *Journal of Personality & Social Psychology, 52,* 81-90.

McCrae, R. R., & Costa Jr, P. T. (2012). *Personality in adulthood: A five-factor theory perspective*. Guilford Press.
McDougall W. (1932). Of the words character and personality. *Character Personality, 1*, 3-16.
Motowidlo, S. J. (2003). Job performance. In W. C. Borman, D. R. Ilgen, & R. J. Klimoski (Eds.), *Handbook of psychology* (Vol. 12; Industrial and organizational psychology, pp. 39-53). Hoboken, NJ: John Wiley & Sons.
Norman W.X. (1963). Toward an adequate taxonomy of personality attributes: Replicated factor structure in peer nomination personality ratings. *Journal of Abnormal & Social Psychology, 66*, 574-583.
Organ, D. W. (1988). *Organizational citizenship behavior: The good soldier syndrome*. Lexington Books/DC Heath and Com.
Organ, D. W. (1997). Organizational citizenship behavior: It's construct clean-up time. *Human performance, 10*(2), 85-97.
Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31*, 673-680.
Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber-security risk. *Computers & Security, 31*, 597-611.
Podsakoff, N. P., Whiting, S. W., Podsakoff, P. M., & Blume, B. D. (2009). Individual-and organizational-level consequences of organizational citizenship behaviors: A meta-analysis. *Journal of Applied Psychology, 94*(1), 122-141.
Raykov, T. (1997). Estimation of composite reliability for congeneric measures. *Applied Psychological Measurement, 21*(2), 173-184.
Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of management journal, 38*(2), 555-572.
Sackett, P. R. (2002). The structure of counterproductive work behaviors: Dimensionality and relationships with facets of job performance. *International Journal of Selection and Assessment, 10*(1-2), 5-11.
Sackett, P. R., & DeVore, C. J. (2001). Counterproductive behaviors at work. *Handbook of Industrial, Work, and Organizational Psychology, 1*, 145-164.
Smith, C. A., Organ, D. W., & Near, J. P. (1983). Organizational citizenship behavior: Its nature and antecedents. *Journal of Applied Psychology, 68*(4), 653-663.
Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.
Steiger, J. H. (1980). Tests for comparing elements of a correlation matrix. *Psychological Bulletin, 87*, 245-251.
Symantec, & Ponemon (2009). More than half of ex-employees admit to stealing company data according to new study. Press release by Symantec Corporation and Ponemon Institute. Retrieved from http://www.symantec.com/about/news/release/article.jsp?prid=20090223_01.
Van Dyne, L., Cummings, L. L., & Parks, J. M. (1995). Extrarole behaviors: In pursuit of construct and definitional clarity. In L. L. Cummings & B. M. Staw (Eds.), *Research in organizational behavior* (Vol. 17, pp. 215-285), Greenwich, CT: JAI Press.
Van Kessel, P. (2008). Moving beyond compliance: Ernst & Young 2008 global information security survey. Retrieved from http://www.ncc.co.uk/article/?articleid=15619.
Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from

habit and protection motivation theory. *Information & Management*. *49.* 190-198.
Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101-105.
Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3-7.
Williams, L. J., & Anderson, S. E. (1991). Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. *Journal of Management*, *17*(3), 601-617.

Tables

Table 1. Summary of Current Security Behavior Taxonomies

Reference	Focus	Categories of Behavior	Dimensions	Range of Behavior
Loch, Carr, and Warkentin (1992)	Threats	None	Source Perpetrator Intention Consequences	Internal – External Human or Non-Human Intentional or Accidental Disclosure of information – Denial of Service
Im and Baskerville (2005)	Threats	None	Intention Mode Motive	Deliberate or Accidental Physical-Virtual Fraud, Espionage, Vandalism
Stanton, Stam, Mastrangelo, and Jolton (2005)	End User Security Behaviors	Intentional destruction Detrimental misuse Dangerous tinkering Naïve mistakes Aware assurance Basic hygiene	User expertise User intentions	Little expertise – expert knowledge Benevolent – Malicious
Guo (2013)	Employee (end user and IS) security-related behaviors	Security assurance Security compliant Security risk-taking Security damaging	Intentionality Motive Expertise Role Job relatedness Consequence Action Rule	Intentional or Unintentional Beneficial – Malicious Low – High End Users or IS People N/A Improve Security – Damage Action or Inaction Organizational Policy or Law

Table 2. Research Question and Hypothesized Relationships

Cyber-Security Behaviors	Research Question 1	What is the underlying factor structure of cyber-security behaviors?
Security Assurance Behaviors	Hypothesis 1a	Conscientiousness will be positively related to security assurance behaviors.
	Hypothesis 1b	Conscientiousness will predict security assurance behaviors, such that individuals high in conscientiousness will engage in more security assurance behaviors than individuals low in conscientiousness.
	Hypothesis 1c	Agreeableness will be positively related to security assurance behaviors.
	Hypothesis 1d	Agreeableness will predict security assurance behaviors, such that individuals high in agreeableness will engage in more security assurance behaviors than individuals low in agreeableness.
	Hypothesis 1e	Openness to Experience will be positively related to security assurance behaviors.
	Hypothesis 1f	Openness to Experience will predict security assurance behaviors, such that individuals high in openness to experience will engage in more security assurance behaviors than individuals low in openness to experience.
Security Compliance Behaviors	Hypothesis 2a	Conscientiousness will be positively related to security compliance behaviors.
	Hypothesis 2b	Conscientiousness will predict security compliance behaviors, such that individuals high in conscientiousness will engage in more security compliance behaviors than individuals low in conscientiousness.
Security Risk Behaviors	Hypothesis 3a	Conscientiousness will be negatively related to security risk behaviors.
	Hypothesis 3b	Conscientiousness will predict security risk behaviors, such that individuals low in conscientiousness will engage in more security risk behaviors than individuals high in conscientiousness.

Table 2, continued. Research Question and Hypothesized Relationships

Security Damaging Behaviors	Hypothesis 4a	Conscientiousness will be negatively related to security damaging behaviors.
	Hypothesis 4b	Conscientiousness will predict security damaging behaviors, such that individuals low in conscientiousness will engage in more security damaging behaviors than individuals high in conscientiousness.
	Hypothesis 4c	Agreeableness will be negatively related to security damaging behaviors.
	Hypothesis 4d	Agreeableness will predict security damaging behaviors, such that individuals low in agreeableness will engage in more security damaging behaviors than individuals high in agreeableness.
	Hypothesis 4e	Emotional Stability will be negatively related to security damaging behaviors.
	Hypothesis 4f	Emotional Stability will predict security damaging behaviors, such that individuals low in emotional stability will engage in more security damaging behaviors than individuals high in emotional stability.
Organizational Citizenship Behaviors	Hypothesis 5a	Organizationally directed organizational citizenship behaviors will be positively related to security assurance behaviors.
	Hypothesis 5b	Organizationally directed organizational citizenship behaviors will be positively related to security compliance behaviors.
	Hypothesis 5c	Security assurance and security compliance behaviors will be more strongly related to organizationally directed citizenship behaviors than interpersonally directed citizenship behaviors.
Counterproductive Work Behaviors	Hypothesis 6a	Organizationally directed counterproductive work behaviors will be positively related to security risk behaviors.
	Hypothesis 6b	Organizationally directed counterproductive work behaviors will be positively related to security damaging behaviors.
	Hypothesis 6c	Security risk and security damaging behaviors will be more strongly related to organizational deviance than interpersonal deviance.

Table 3. Descriptive Statistics for Cyber-Security Scale Items

Item		Mean	SD	Min	Max	% Who Performed Behavior
SAB1	Monitored your work computer for signs of a virus or malware	4.20	2.323	1	7	75.3%
SAB2	Immediately deleted suspicious emails in your work email without reading them	4.47	2.289	1	7	79.5%
SAB3	Refused to tell anyone your work ID or password	3.77	2.391	1	7	70.2%
SAB4	Used a secure password for your work computer. (i.e. a password containing a combination of letters, numbers, and symbols)	5.52	1.943	1	7	93.1%
SAB5	Changed your password more frequently than your employer requires.	2.29	1.760	1	7	43.8%
SAB6	Went above and beyond what is required of you in order to protect your work information.	3.96	2.190	1	7	76.1%
SCB1	Followed the information security policies and practices at work	6.00	1.649	1	7	95.6%
SCB2	Used the information security technology provided to you at work.	4.90	2.315	1	7	81.8%
SCB3	Used good information security practices at work.	5.81	1.758	1	7	94.8%
SCB4	Complied with organizational information security policies to protect the organization's information systems.	5.17	2.282	1	7	83.9%
SRB1	Written your work password on a piece of paper and left it where others might see it.	1.79	1.482	1	7	28.1%
SRB2	Chosen relatively simple passwords for your work computer.	2.43	1.817	1	7	50.1%
SRB3	Shared your work account user name or password with a friend or coworker.	1.64	1.352	1	7	24.3%
SRB4	Used your social security number as your password.	1.28	.954	1	7	10.3%
SRB5	Copied work information onto a personal USB drive to do work at home.	2.12	1.771	1	7	35.1%
SRB6	Installed unauthorized software from the internet onto your work computer without permission from your employer.	1.59	1.241	1	7	23.9%
SRB7	Walked away from your computer without locking it first.	1.33	.977	1	7	75.3%
SDB1	Attempted to crack the password on the firewall your company has set in place to assess prohibited websites while at work.	1.25	.846	1	7	12.6%
SDB2	Introduced a Trojan horse program into your company’s network.	1.36	1.082	1	7	9.6%
SDB3	Used a file decryption program to discover the contents of a file containing information you are not authorized to see.	1.33	1.006	1	7	12.6%
SDB4	Used you company email to send spam messages for personal gain.	1.62	1.335	1	7	11.7%
SDB5	Communicated confidential information on an unsecured network.	4.09	2.336	1	7	21.2%
SDB6	Intentionally disclosed confidential company information to unauthorized sources.	1.27	.848	1	6	11.0%

Table 4. Exploratory Factor Analysis Loadings

	Factors			
	1	2	3	4
Security Assurance Behaviors				
Monitored your work computer for signs of a virus or malware				0.486
Changed your password more frequently than your employer requires.				0.402
Went above and beyond what is required of you in order to protect your work information.				0.512
Security Compliance Behaviors				
Used a secure password for your work computer. (i.e. a password containing a combination of letters, numbers, and symbols)		0.679		
Followed the information security policies and practices at work		0.727		
Used the information security technology provided to you at work.		0.536		
Used good information security practices at work.		0.738		
Complied with organizational information security policies to protect the organization's information systems.		0.608		
Security Risk Behaviors				
Written your work password on a piece of paper and left it where others might see it.			0.402	
Chosen relatively simple passwords for your work computer.			0.668	
Shared your work account user name or password with a friend or coworker.			0.452	
Walked away from your computer without locking it first.			0.453	
Security Damaging Behaviors				
Used your social security number as your password.	0.895			
Copied work information onto a personal USB drive to do work at home.	0.414			
Installed unauthorized software from the internet onto your work computer without permission from your employer.	0.615			
Attempted to crack the password on the firewall your company has set in place to assess prohibited websites while at work.	0.845			
Introduced a Trojan horse program into your company’s network.	0.868			
Used a file decryption program to discover the contents of a file containing information you are not authorized to see.	0.805			
Used you company email to send spam messages for personal gain.	0.814			
Communicated confidential information on an unsecured network.	0.494			
Intentionally disclosed confidential company information to unauthorized sources.	0.825			

Table 5. Confirmatory Factor Analysis Loadings

Factor and Item	Loading	CR
Security Assurance Behaviors		0.63
Monitored your work computer for signs of a virus or malware.	0.53	
Changed your password more frequently than your employer requires.	0.40	
Went above and beyond what is required of you in order to protect your work information.	0.66	
Security Compliance Behaviors		0.75
Used a secure password for your work computer. (i.e. a password containing a combination of letters, numbers, and symbols)	0.50	
Followed the information security policies and practices at work.	0.71	
Used the information security technology provided to you at work.	0.53	
Used good information security practices at work.	0.65	
Complied with organizational information security policies to protect the organization's information systems.	0.63	
Security Risk Behaviors		0.63
Written your work password on a piece of paper and left it where others might see it.	0.60	
Chosen relatively simple passwords for your work computer.	0.46	
Shared your work account user name or password with a friend or coworker.	0.72	
Walked away from your computer without locking it first.*	0.18	
Security Damaging Behaviors		0.89
Used your social security number as your password.	0.81	
Copied work information onto a personal USB drive to do work at home.	0.34	
Installed unauthorized software from the internet onto your work computer without permission from your employer.	0.59	
Attempted to crack the password on the firewall your company has set in place to assess prohibited websites while at work.	0.74	
Introduced a Trojan horse program into your company’s network.	0.77	
Used a file decryption program to discover the contents of a file containing information you are not authorized to see.	0.68	
Used you company email to send spam messages for personal gain.	0.81	
Communicated confidential information on an unsecured network.	0.58	
Intentionally disclosed confidential company information to unauthorized sources.	0.77	

Notes: *Item removed from final scale. CR = Composite Reliability

Table 6. Model Fit Indices

Model	Model Description	Satorra-Bentler Scaled χ^2	*df*	CFI	TLI	RMSEA (90% CI)	SRMR
1	Four Factor Model	346.815**	183	0.86	0.84	.06(.051-.07)	0.07
2	Four Factor Model with SRB7 removed	290.99**	164	0.89	0.87	.057(.046-.068)	0.065

Notes: $^{*}p < .05$, $^{**}p < .01$. CFI = comparative fit index; TLI – Tucker-Lewis index of fit; RMSEA = root mean square error of approximation; SRMR = Standardized root mean square residual.

Table 7. Means, Standard Deviations, Skewness, and Kurtosis of Study Variables

	M	SD	Skewness	Kurtosis
1. Age	36.15	11.86	.91	.28
2. Gender	1.53	0.50	-.11	-2.00
3. Education	5.02	1.70	-.27	-.70
4. Computer Use (Hours)	25.73	14.35	-.09	-.83
5. Job Tenure (Years)	5.21	4.75	1.90	4.75
6. Job Title (IT/non-IT)	0.07	0.25	3.53	10.52
7. Severity of Punishment	3.73	0.94	-.75	.30
8. Extraversion	2.93	0.82	.14	-.40
9. Agreeableness	3.87	0.64	-.40	-.15
10. Conscientiousness	3.82	0.62	-.32	-.04
11. Emotional Stability	3.30	0.68	-.14	-.42
12. Openness to Experience	3.78	0.61	-.17	-.18
13. OCB-I	3.65	0.67	-.14	.04
14. OCB-O	4.08	0.58	-.56	-.26
15. Interpersonal Deviance	1.47	0.66	2.04	4.22
16. Organizational Deviance	1.64	0.61	1.61	3.03
17. Security Assurance Behaviors	3.48	1.50	.25	-.42
18. Security Compliance Behaviors	5.48	1.39	-.85	.16
19. Security Risk Behaviors	1.95	1.18	1.41	1.49
20. Security Damaging Behaviors	1.46	0.81	2.66	7.28

Note: Job Title is dichotomized

Table 8. Intercorrelations Among Study Variables

	1	2	3	4	5	6	7	8	9	10
1. Age	-									
2. Gender	.05	-								
3. Education	.09	.00	-							
4. Computer Use (Hours)	.00	-.01	.14**	-						
5. Job Tenure (Years)	.42***	.00	.02	.07	-					
6. Job Title (IT/non-IT)	.00	-.14**	-.01	.16**	.02	-				
7. Severity of Punishment	.00	-.01	-.09	-.01	-.03	.00	(.88)			
8. Extraversion	.05	.04	.01	-.04	.04	-.02	.01	(.89)		
9. Agreeableness	.23***	.29***	.01	-.04	.11*	-.05	.20***	.30***	(.87)	
10. Conscientiousness	.23***	.19***	.15**	.06	.15**	-.03	.17***	.11*	.39***	(.84)
11. Emotional Stability	.25***	-.15**	.16**	.04	.12*	.06	.09*	.28***	.26***	.40***
12. Openness to Experience	.04	.07	.07	.04	-.05	-.05	.09	.22***	.35***	.33***
13. OCB-I	.05	.18***	-.05	.03	.09	-.06	.21***	.13**	.36***	.35***
14. OCB-O	.27***	.15**	.01	.00	.09	-.05	.29***	-.02	.42***	.48***
15. Interpersonal Deviance	-.22***	-.23***	-.07	.00	-.05	-.01	-.11*	.00	-.40***	-.40***
16. Organizational Deviance	-.23***	-.16**	-.04	.01	-.08	-.02	-.14**	-.03	-.40***	-.50***
17. Security Assurance Behaviors	.09	-.07	-.01	.01	.10*	.08	.20***	.07	.15**	.18***
18. Security Compliance Behaviors	.20***	.04	.13**	.14**	.07	.02	.19***	.03	.29***	.27***
19. Security Risk Behaviors	-.13**	.00	.00	-.03	-.01	-.04	-.15**	.08	-.14**	-.21***
20. Security Damaging Behaviors	-.22***	-.21***	-.04	-.02	.00	.02	-.12*	.04	-.29***	-.32***

Notes: N = 450-477; Job Title is dichotomized; *p<.05, **p<.01, ***p<.001

Table 8 continued. Intercorrelations Among Study Variables

	11	12	13	14	15	16	17	18	19	20
1. Age										
2. Gender										
3. Education										
4. Computer Use (Hours)										
5. Job Tenure (Years)										
6. Job Title (IT/non-IT)										
7. Severity of Punishment										
8. Extraversion										
9. Agreeableness										
10. Conscientiousness										
11. Emotional Stability	(.79)									
12. Openness to Experience	.24***	(.84)								
13. OCB-I	.08	.29***	(.78)							
14. OCB-O	.27***	.29***	.34***	(.69)						
15. Interpersonal Deviance	-.24***	-.21***	-.13**	-.56***	(.91)					
16. Organizational Deviance	-.29***	-.20***	-.22***	-.64***	.83***	(.90)				
17. Security Assurance Behaviors	.19***	.11*	.18***	.15**	.00	-.06	(.63)			
18. Security Compliance Behaviors	.21***	.27***	.22***	.44***	-.34***	-.31***	.25***	(.75)		
19. Security Risk Behaviors	-.18***	-.16***	.00	-.40***	.43***	.48***	-.02	-.24***	(.63)	
20. Security Damaging Behaviors	-.11*	-.21***	-.12*	-.55***	.61***	.61***	.16***	-.25***	.55***	(.89)

Notes: N = 450-477; Job Title is dichotomized; *p<.05, **p<.01, ***p<.001

Table 9. Regression Results: Predicting Security Assurance Behaviors

Model	1: Conscientiousness	2: Agreeableness	3: Openness to Experience
Step 1: Controls			
Age	.09*	.09	.10*
Gender	-.07	-.08	-.07
Computer Use	.00	.01	.02
Severity of Punishment	.20***	.19***	.20***
Step 1 R^2	.06***	.05***	.05***
Step 2: Direct Effects			
Age	.06	.06	.09*
Gender	-.10*	-.11*	-.08
Computer Use	.00	.02	.02
Severity of Punishment	.18***	.16**	.19***
1. Conscientiousness	.15**		
2. Agreeableness		.14**	
3. Openness to Experience			.10*
Total F	7.23***	6.30***	5.976***
Total R^2	.08**	.07**	.06
ΔR^2	0.02	0.02	0.01

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

Table 10. Regression Results: Predicting Security Compliance Behaviors

Model	1: Conscientiousness
Step 1: Controls	
Age	.21***
Gender	.03
Computer Use	.14**
Severity of Punishment	.18***
Step 1 R^2	.10***
Step 2: Direct Effects	
Age	.17***
Gender	-.01
Computer Use	.13**
Severity of Punishment	.15**
1. Conscientiousness	.19***
Total F	13.45***
Total R^2	.13
ΔR^2	.03***

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

Table 11. Regression Results: Predicting Security Risk Behaviors

Model	1: Conscientiousness
Step 1: Controls	
Age	-.13**
Gender	.01
Computer Use	-.03
Severity of Punishment	-.14**
Step 1 R^2	.04**
Step 2: Direct Effects	
Age	-.09
Gender	.04
Computer Use	-.02
Severity of Punishment	-.10*
1. Conscientiousness	-.18***
Total F	6.17***
Total R^2	.06***
ΔR^2	0.03

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

Table 12. Regression Results: Predicting Security Damaging Behaviors

Model	1: Conscientiousness	2: Agreeableness	3: Openness to Experience
Step 1: Controls			
Age	-.20***	-.22***	-.21***
Gender	-.19***	-.19***	-.17***
Computer Use	-.03	-.01	.00
Severity of Punishment	-.11*	-.12**	-.12**
Step 1 R^2	.09***	.10***	.09***
Step 2: Direct Effects			
Age	-.15**	-.18***	-.19***
Gender	-.15**	-.13**	-.18***
Computer Use	.00	-.01	.00
Severity of Punishment	-.06	-.08	-.11*
1. Conscientiousness	-.25***		
2. Agreeableness		-.19***	
3. Emotional Stability			-.08
Total F	15.56***	13.66***	9.23***
Total R^2	.15***	.13***	.09
ΔR^2	0.06	0.03	0.01

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

Figures

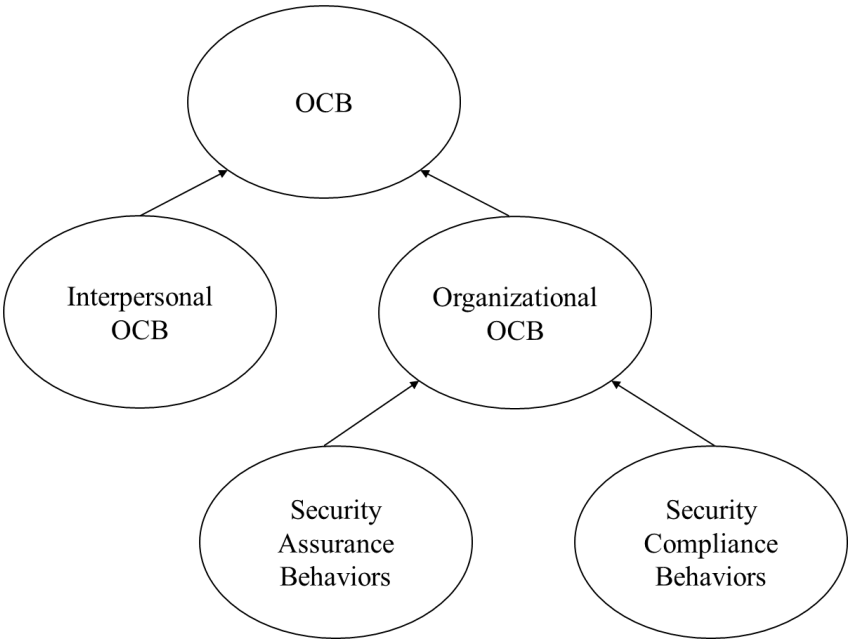

Figure 1. *Conceptual relationship between cyber behaviors and organizational citizenship behaviors.*

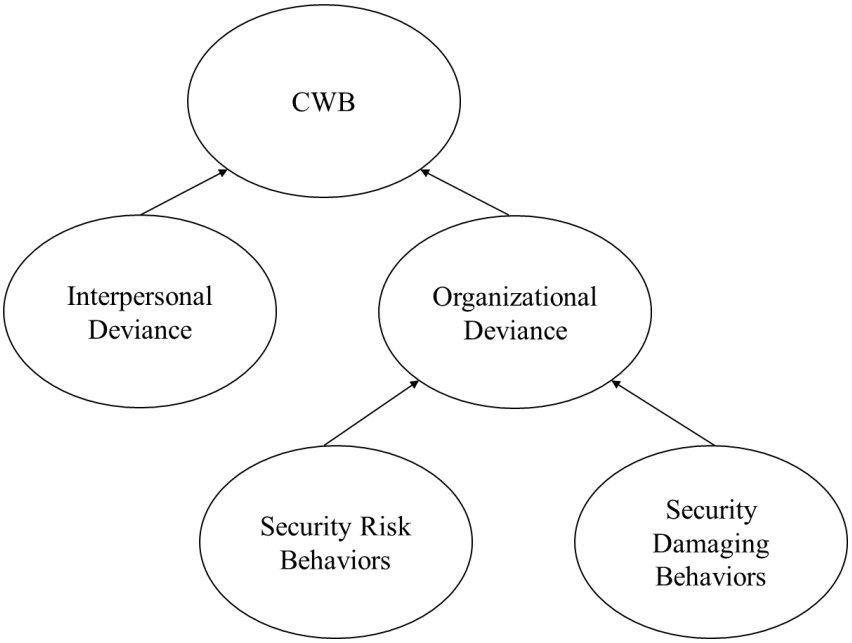

Figure 2. *Conceptual relationship between cyber behaviors and counterproductive work behaviors.*

Appendices

Appendix A: Cyber-Security Behavior Scale

Please indicate the frequency in which these you have engaged in each of the following behaviors in the past year.

Response Options: 1 = "Never"; 2 = "Once a Year"; 3 = "Twice a Year"; 4 = "Several times a year"; 5 = "Monthly"; 6 = "Weekly"; 7 = "Daily"

Behavior		Items	Source
Security Assurance	SAB1	Monitored your work computer for signs of a virus or malware	Stanton et al (2005)
	SAB2	Immediately deleted suspicious emails in your work email without reading them	Yoon et al (2012)
	SAB3	Refused to tell anyone your work ID or password	Yoon et al (2012)
	SAB4	Used a secure password for your work computer. (i.e. a password containing a combination of letters, numbers, and symbols)	Stanton et al (2005)
	SAB5	Changed your password more frequently than your employer requires.	Self-Developed
	SAB6	Went above and beyond what is required of you in order to protect your work information.	Self-Developed
Security Compliance	SCB1	Followed the information security policies and practices at work	Hu et al. (2012)
	SCB2	Used the information security technology provided to you at work.	Hu et al. (2012)
	SCB3	Used good information security practices at work.	Hu et al. (2012)
	SCB4	Complied with organizational information security policies to protect the organization's information systems.	Herath & Rao (2009)
Security Risk	SRB1	Written your work password on a piece of paper and left it where others might see it.	Stanton et al (2005)
	SRB2	Chosen relatively simple passwords for your work computer.	Stanton et al (2005)
	SRB3	Shared your work account user name or password with a friend or coworker.	Stanton et al (2005)
	SRB4	Used your social security number as your password.	Stanton et al (2005)
	SRB5	Copied work information onto a personal USB drive to do work at home.	Guo et al (2011)

	SRB6	Installed unauthorized software from the internet onto your work computer without permission from your employer.	Guo et al (2011)
	SRB7	Walked away from your computer without locking it first.	Self-Developed
Security Damaging	SDB1	Attempted to crack the password on the firewall your company has set in place to assess prohibited websites while at work.	Self-Developed
	SDB2	Introduced a Trojan horse program into your company's network.	Stanton et al (2005)
	SDB3	Used a file decryption program to discover the contents of a file containing information you are not authorized to see.	Stanton et al (2005)
	SDB4	Used you company email to send spam messages for personal gain.	Stanton et al (2005)
	SDB5	Communicated confidential information on an unsecured network.	Self-Developed
	SDB6	Intentionally disclosed confidential company information to unauthorized sources.	Self-Developed

Appendix B: Big Five Personality Scales

On the following pages, there are phrases describing people's behaviors. Please use the rating scale below to describe how accurately each statement describes *you*. Describe yourself as you generally are now, not as you wish to be in the future. Describe yourself as you honestly see yourself, in relation to other people you know of the same sex as you are, and roughly your same age. So that you can describe yourself in an honest manner, your responses will be kept in absolute confidence. Please read each statement carefully, and then select an option on the scale.

Response Options: 1 = "Very Inaccurate"; 2 = "Moderately Inaccurate"; 3 = "Neither Inaccurate nor Accurate"; 4 = "Moderately Accurate"; 5 = "Very Accurate"

Neuroticism

1. Am often down in the dumps.
2. Dislike myself
3. Often feel blue
4. Have frequent mood swings.
5. Panic easily.
6. Am filled with doubts about things.
7. Feel threatened easily.
8. Get stressed out easily.
9. Fear for the worst.
10. Worry about things.
11. Seldom feel blue.
12. Feel comfortable with myself.
13. Rarely get irritated.
14. Am not easily bothered by things.
15. Am very pleased with myself.
16. Am relaxed most of the time.
17. Seldom get mad.
18. Am not easily frustrated.
19. Remain calm under pressure.
20. Rarely lose my composure.

Extraversion

1. Feel comfortable around people.
2. Make friends easily.
3. Am skilled in handling social situations.
4. Am the life of the party.
5. Know how to captivate people.
6. Start conversations.
7. Warm up quickly to others.
8. Talk to a lot of different people at parties.
9. Don't mind being the center of attention.
10. Cheer people up.

11. Have little to say.
12. Keep in the background.
13. Would describe my experiences as somewhat dull.
14. Don't like to draw attention to myself.
15. Don't talk a lot.
16. Avoid contacts with others.
17. Am hard to get to know.
18. Retreat from others.
19. Find it difficult to approach others.
20. Keep others at a distance.

Openness to Experience

1. Believe in the importance of art.
2. Have a vivid imagination.
3. Tend to vote for liberal political candidates.
4. Carry the conversation to a higher level.
5. Enjoy hearing new ideas.
6. Enjoy thinking about things.
7. Can say things beautifully.
8. Enjoy wild flights of fantasy.
9. Get excited by new ideas.
10. Have a rich vocabulary.
11. Am not interested in abstract ideas.
12. Do not like art.
13. Avoid philosophical discussions.
14. Do not enjoy going to art museums.
15. Tend to vote for conservative political candidates.
16. Do not like poetry.
17. Rarely look for a deeper meaning in things.
18. Believe that too much tax money goes to support artists.
19. Am not interested in theoretical discussions.
20. Have difficulty understanding abstract ideas.

Agreeableness

1. Have a good word for everyone.
2. Believe that others have good intentions.
3. Respect others.
4. Accept people as they are.
5. Make people feel at ease.
6. Am concerned about others.
7. Trust what people say.
8. Sympathize with others' feelings.
9. Am easy to satisfy.
10. Treat all people equally.

11. Have a sharp tongue.
12. Cut others to pieces.
13. Suspect hidden motives in others.
14. Get back at others.
15. Insult people.
16. Believe that I am better than others.
17. Contradict others.
18. Make demands on others.
19. Hold a grudge.
20. Am out for my own personal gain.

Conscientiousness

1. Am always prepared.
2. Pay attention to details.
3. Get chores done right away.
4. Carry out my plans.
5. Make plans and stick to them.
6. Complete tasks successfully.
7. Do things according to a plan.
8. Am exacting in my work.
9. Finish what I start.
10. Follow through with my plans.
11. Waste my time.
12. Find it difficult to get down to work.
13. Do just enough work to get by.
14. Don't see things through.
15. Shirk my duties.
16. Mess things up.
17. Leave things unfinished.
18. Don't put my mind on the task at hand.
19. Make a mess of things.
20. Need a push to get started.

Appendix C: Organizational Citizenship Behavior Scales

Please indicate the frequency in which these you have engaged in each of the following behaviors in the past year.

Response Options: 1 = "Never"; 2 = "Rarely"; 3 = "Sometimes"; 4 = "Most of the Time"; 5 = "Always"

Interpersonally Directed OCBs

1. I help others who have been absent.
2. I help others who have heavy workloads.
3. I assist my supervisor with his/her work when not asked.
4. I take time to listen to co-workers' problems and worries.
5. I go out of my way to help new employees.
6. I pass along information to co-workers.

Organizationally Directed OCBs

1. My attendance to work is about the norm.
2. I give advance notice when unable to come to work.
3. I take underserved work breaks.
4. I spend a great deal of time with personal phone conversations.
5. I complain about insignificant things at work.
6. I adhere to informal rules devised to maintain order.

Appendix D: Counterproductive Work Behavior Scales

Please indicate the frequency in which these you have engaged in each of the following behaviors in the past year.

Response Options: 1 = "Never"; 2 = "Rarely"; 3 = "Sometimes"; 4 = "Most of the Time"; 5 = "Always"

Interpersonally Directed CWBs

1. Made fun of someone at work.
2. Said something hurtful to someone at work.
3. Made an ethnic, religious, or racial remark at work.
4. Cursed at someone at work.
5. Played a mean prank on someone at work.
6. Acted rudely toward someone at work.
7. Publicly embarrassed someone at work.

Organizationally Directed OCBs

1. Taken property from work without permission.
2. Spent too much time fantasizing or daydreaming instead of working.
3. Falsified a receipt to get reimbursed for more money than you spent on business expenses.
4. Taken an additional or longer break than is acceptable at your workplace.
5. Come in late to work without permission.
6. Littered your work environment.
7. Neglected to follow your boss's instructions.
8. Intentionally worked slower than you could have worked.
9. Discussed confidential company information with an unauthorized person.
10. Used an illegal drug or consumed alcohol on the job.
11. Put little effort into your work.
12. Dragged out work in order to get overtime.

Appendix E: Severity of Punishment Scale

Please indicate the extent to which you agree with the following statements when thinking about **your organization**.

Response Options: 1 = “Strongly Disagree”; 2 = “Disagree”; 3 = “Neither Agree nor Disagree”; 4 = “Agree”; 5 = “Strongly Agree”

1. The organization disciplines employees who break information security rules
2. My organization terminates employees who repeatedly break security rules
3. If I were caught violating organization information security policies, I would be severely punished

Appendix F: Demographics Questions

What is your gender?

- Male
- Female

What is your age in years? _____

Please indicate how long you have held your current job (in years). _____

On average, how many hours do you work per week? _____

How many hours per week do you use a computer at work? _____

What is your job title? _____

Please indicate your highest level of education

- Some high school
- High school diploma/GED
- Some college
- Trade/technical/vocational training
- Associate's degree
- Bachelor's degree
- Master's degree
- Professional degree
- Doctoral degree

Appendix G: Institutional Review Board Approval Letter

October 20, 2015

Rachel Dreibelbis
Psychology
4202 East Fowler Avenue
PCD4118G
Tampa, FL 33620

RE: **Exempt Certification**
IRB#: Pro00024125
Title: The Nature of Cyber Security in the Workplace

Dear Ms. Dreibelbis:

On 10/19/2015, the Institutional Review Board (IRB) determined that your research meets criteria for exemption from the federal regulations as outlined by 45CFR46.101(b):

(2) Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless:
(i) information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

Approved Items:

Study Protocol

Informed Consent Document Revised

As the principal investigator for this study, it is your responsibility to ensure that this research is conducted as outlined in your application and consistent with the ethical principles outlined in the Belmont Report and with USF HRPP policies and procedures.

Please note, as per USF HRPP Policy, once the Exempt determination is made, the application is closed in ARC. Any proposed or anticipated changes to the study design that was previously declared exempt from IRB review must be submitted to the IRB as a new study prior to initiation

of the change. However, administrative changes, including changes in research personnel, do not warrant an amendment or new application.

Given the determination of exemption, this application is being closed in ARC. This does not limit your ability to conduct your research project.

We appreciate your dedication to the ethical conduct of human subject research at the University of South Florida and your continued commitment to human research protections. If you have
any questions regarding this matter, please call 813-974-5638.

Sincerely,

John Schinka, Ph.D., Chairperson
USF Institutional Review Board