March 2018

Better Safe than Sorry: The Relationship Between Locus of Control, Perception of Risk, and Cyber Misbehaviors

Kim Johnson
University of South Florida, kimj@mail.usf.edu

Follow this and additional works at: https://scholarcommons.usf.edu/etd
Part of the Psychology Commons

Scholar Commons Citation

This Thesis is brought to you for free and open access by the Graduate School at Scholar Commons. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Scholar Commons. For more information, please contact scholarcommons@usf.edu.
Better Safe than Sorry:
The Relationship Between Locus of Control, Perception of Risk, and Cyber Misbehaviors

by

Kim Johnson

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 Coovert, Ph.D.
Walter Borman, Ph.D.
Chad Dube, Ph.D.

Date of Approval:
December 4, 2017

Keywords: cybersecurity, cyber safety, cyber risk, information security

Copyright @ 2017, Kim Johnson
TABLE OF CONTENTS

List of Tables ........................................................................................................................................ iii

List of Figures ......................................................................................................................................... iv

Abstract .................................................................................................................................................. v

Chapter One: Introduction ................................................................................................................................. 1

  Behavior in Organizations ............................................................................................................................... 3
    Job Attitudes ........................................................................................................................................ 4
    Affect and Emotion ................................................................................................................................. 5
    Organizational Justice ............................................................................................................................. 6
    Leadership ............................................................................................................................................ 8
    Workplace Teams .................................................................................................................................... 10
    Motivation ........................................................................................................................................... 11
  Organizational Socialization and Person-Environment Fit ........................................................................... 13
  Organizational Culture and Climate ........................................................................................................... 14
  Health and Safety .................................................................................................................................... 15
  Work-Family Conflict and Balance ........................................................................................................... 16
  Turnover .................................................................................................................................................. 18
  Organizational Citizenship Behavior .......................................................................................................... 19
  Counterproductive Work Behavior ............................................................................................................ 19
  Overall Organizational Behavior ............................................................................................................. 20

Cyber-Threats Defined ................................................................................................................................. 22

Training in Organizations .............................................................................................................................. 23

Deterring Cyber Misbehaviors Through Training ....................................................................................... 24

Training Delivery Methods ......................................................................................................................... 25

Attitude Change ......................................................................................................................................... 27

Influencing Cybersecurity Attitudes ............................................................................................................ 29

Locus of Control ......................................................................................................................................... 30

  Hypothesis 1 .......................................................................................................................................... 33

Risk and Risk Perception ............................................................................................................................... 33

Theories Related to Risk Perception and Risk Tolerance ............................................................................. 35

  Protection Motivation Theory .................................................................................................................... 35
  Situated Rationality Theory ....................................................................................................................... 36
  Risk Compensation Theory ...................................................................................................................... 37
  Social Control Theory ............................................................................................................................... 37
  Social Action Theory ................................................................................................................................. 38

Cyber Behaviors Defined ............................................................................................................................... 39

Risk Through Misbehavior ............................................................................................................................ 44

Locus of Control and Risk Perception ........................................................................................................... 45
LIST OF TABLES

Table 1: Fit Statistics/Model Comparisons: Locus of Control ................................................. 117

Table 2: Fit Statistics/Model Comparisons: Sensation Seeking ................................................. 118
LIST OF FIGURES

Figure 1: Model 1: Locus of Control Associated with Cyber Misbehavior ........................................33
Figure 2: Model 2: Risk Perception as a Mediator .........................................................................46
Figure 3: Model 3: Risk Perception as a Moderator .......................................................................47
Figure 4: Model 4: Locus of Control Associated with Risk Perception and Cyber Misbehavior ..........................................................48
Figure 5: Model 5: Pathways Between All Constructs ..................................................................48
Figure 6: Exploratory Model A: Cyber Risk Perception as Mediator ...........................................50
Figure 7: Exploratory Model B: Cyber Misbehavior as Mediator ..............................................51
Figure 8: Standardized Estimates for Model 1 ..............................................................................63
Figure 9: Standardized Estimates for Model 2 ..............................................................................65
Figure 10: Standardized Estimates for Model 3 .............................................................................66
Figure 11: Standardized Estimates for Model 4 .............................................................................67
Figure 12: Standardized Estimates for Model 5 .............................................................................68
Figure 13: Standardized Estimates for Exploratory Model A .......................................................70
Figure 14: Standardized Estimates for Exploratory Model B .......................................................71
Figure 15: Standardized Estimates for Exploratory Model C .......................................................72
Figure 16: Standardized Estimates for Exploratory Model D .......................................................73
Abstract

Information security is of vital importance to organizations. Breaches in security very often stem from behaviors of the system operator. Cyber misbehaviors on the part of employees can have devastating repercussions on the well-being of an organization. Up to now, research has mainly focused on how to protect information systems from outside attack, and only recently have researchers turned to the part the operator plays in keeping the systems safe. The present study investigated some individual differences that may play a role in people’s cyber behavior. The purpose of the study was to determine if locus of control was related to an individual’s perception of cyber risk and likelihood of engaging in cyber misbehaviors. Internal locus of control was found to be associated with higher perception of cyber risk, and higher cyber risk perception was found to lead to fewer cyber misbehaviors. The trait sensation seeking was also explored but no firm conclusions could be drawn from those results. Gaining an understanding of some of the differences between individuals that make some more likely to commit cyber misbehaviors-- as well as the dynamics behind these relationships—should be greatly beneficial in helping develop deterrents to cyber misbehavior and keeping information systems safer.
CHAPTER ONE:

INTRODUCTION

Decisions are made every minute of every hour of every day in the operation of an organization. Some decisions made by individual employees have seemingly little impact on the performance of the organization--which task to complete first, whether or not to send a follow-up email to a coworker or client, which team member to ask to take the lead on a new project; while other decisions appear to have the potential to make or break a corporation--whether to merge with another company, the best way to transition from one CEO to the next, or how to get a large contract signed. Some decisions are made with a great deal of deliberation while others appear to be more impulsive. Ostensibly it would be the monumental decisions that would have the most effect on the company bottom line, but that is not necessarily always the case. All it takes is for one employee to click on one seemingly innocuous email attachment (for example, promising photos of cute kittens doing adorable things), which releases malware allowing a cyber-thief to download the organization’s sensitive information, and the future of that organization can change dramatically. These small decisions made every day by employees at every level have the potential to have an impact on the company as great as that of any weighty decision made by the CEO.

Never before have organizations faced such circumstances. In the past, small decisions made by lower-level employees had an aggregate effect on the bottom line of the company. Poor but relatively insignificant decisions made at the lowest level of the corporate staffing chain had
the potential to impact the company only if there were enough that were not addressed and corrected. Faulty decisions made by individuals near the top of the organizational chart would have a greater effect on the corporation. With the advent of technology, all of this is changing; any employee with clearance to access the company’s computer system is a potential cyber-threat to the company (Abawajy, 2014).

There is no turning back from the dependence on technology. From storing client information and patient records, to facilitating the exchange of information, to the crafting of strategic military plans, technology plays a vital role in almost every organization. It is nearly impossible to conduct business in the developed world without spending time in cyberspace. Yet there are dangers lurking there. Computer viruses, hackers gaining access to confidential information, denial of service attacks, and other computer security issues are commonplace. The public has almost become inured to reports of yet another security breach affecting millions of people. In 2015 alone, CVS pharmacy had credit card data and personal information stolen for millions of customers, Patreon crowdfunding service had the entirety of its data-- all 15GB of it--stolen and published online, LastPass password manager-- a company whose sole purpose is to keep people more cyber secure-- was hacked, Experion credit agency suffered a breach which led to the theft of data, including social security numbers, for upwards of 15 million T-Mobile customers, a breach at the IRS cost taxpayers approximately $50 million in fraudulent tax returns, as well as the Ashley Madison extramarital dating site’s loss of personal information for 37 million cheating spouses (Whittaker, 2015). For those of us who would never patronize such a site, the last example seems mildly humorous and possibly fair punishment, but if this information were to get into the hands of foreign enemies there could be blackmail and potential for national security leaks. Probably the most frightening security breach of 2015 occurred at the
U.S. Office of Personnel Management, with the theft of the background checks of over 22 million government officials and employees (Whittaker, 2015). Clearly, cybersecurity is an issue of concern for everyone, from patrons, customers, and patients whose information is being compromised, to corporations who stand to lose millions of dollars as well as their less repairable reputation and good name, to government agencies whose sensitive information is a matter of national security.

An incessant battle is being waged by information technology professionals to maintain control over corporate technology and protect information assets against cyber-threat. Despite rapid advancements in security technology, the detection and prevention of malicious or dangerous computer activity often depends on the users’ actions. Technological solutions alone are not the answer when information systems involve human users (Aytes & Connolly, 2004). As Weiderhold (2014) stated, “the human factor remains security’s weakest link in cyberspace,” and according to Schmidt (2012), “human error represents the biggest threat to the ability of [security] technology to protect an enterprise’s communications network.”

With computer error on the part of the employee at the heart of most cyber-threats, it is important to take a close look at the actions of the individual. In order to make the most cyber-secure choices, the employee must first perceive cybersecurity as important. Next, they must know to take the safest actions. Finally, the individual must choose to make cyber-safe decisions. There are many factors and individual traits that may affect these cognitions and behaviors. The purpose of this study is to identify the relationship among some of these individual traits and factors with risky cybersecurity behavior.

**Behavior in Organizations**

Before cyber behaviors and their antecedents can be examined, it is important to look at
behavior in organizations as it normally occurs. There are many facets and dimensions of organizational behavior, any one of which could contribute to or be associated with cyber misbehaviors.

**Job attitudes.** Job attitudes are important because they influence behaviors in the workplace. An individual’s beliefs can come from many sources and are a precursor to attitudes. Attitudes consist of an evaluation of the beliefs that are held, which leads to behavior. Behavior is an intention based on the earlier evaluation (Bono & Patton, 2001). Attitude toward the organization, the job, job tasks, coworkers, and other organizational facets lead to job satisfaction, which is experienced on a continuum (Macey & Schneider, 2008).

Job satisfaction is a multidimensional response to one’s job, and consists of cognitive (evaluative) and affective (emotional) components (Bono & Patton, 2001). Job satisfaction can be measured using a global assessment, as in how a person’s job makes them feel overall; or it can be measured using a facet approach, which is a composite of many different and potentially conflicting feelings about the job (Cooper-Hakin & Viswesvaran, 2005). There are many possible environmental antecedents to job satisfaction, including skill variety, autonomy, task identity and significance, role ambiguity, feedback, and pay, among others. Most supervisors rate pay as the most important predictor of job satisfaction, while most employees rate interest in the work as most important (Bono & Patton, 2001). Personality factors and affect can also influence perceptions of job satisfaction. Situational aspects of the job and individual factors about the person interact to impact attitudes of job satisfaction (Judge, Hulun, and Dalal, 2009).

Job satisfaction is important because it is associated with many outcomes such as job performance, organizational citizenship behaviors, employee engagement, and job commitment. Organizational citizenship behaviors are discretionary behaviors that promote the well-being of
the organization and are beyond the formal requirements of the job (Organ, 1988). Employee engagement consists of interest and enthusiasm regarding the work (Macey & Schneider, 2008). Organizational commitment is the employee’s involvement and loyalty to an organization and is related to intention to remain at the job (Le et al., 2010).

Job attitude, or the “A-Factor” as Harrison, Newman, and Roth (2006) term it, can be modeled with overall job attitude leading to higher job satisfaction and organizational commitment, and with overall job attitude also associated with individual effectiveness—positively with the facets focal performance and contextual performance, and negatively with the facets lateness, absenteeism, and turnover (Harrison, Newman, & Roth, 2006).

Bulgurcu, Cavusoglu, and Benbasat (2009) found that employees’ attitudes toward security compliance are related to their intention to comply, illustrating the importance of attitude regarding cyber behavior. As an antecedent to behavior, attitude always plays a vital role in any study of behavior.

**Affect and Emotion.** Job attitudes are all at least moderately related to affect and emotion (Thoreson et al., 2003). Emotion is an adaptive function that helps a person respond to the environment, and is both a subjective feeling state and an action inducer (Fredrickson, 2001). Positive affect is related to the experiencing of a pleasant mood, with feelings such as joy, interest, enthusiasm, and alertness (Watson, Clark, & Tellegen, 1988). Negative affect reflects emotional distress, and includes moods like fear, sadness, anger and guilt (Watson, Clark, & Tellegen, 1988). State affect is a temporary experience of positive or negative affect. Trait affect is an affective disposition in either a positive or negative direction; a person who is generally happy and upbeat would be said to exhibit positive trait affect (Beal, Weiss, Barros, & MacDermid, 2005).
Sometimes a person’s job will require them to exhibit an emotion they may not necessarily feel, such as a customer service representative having to be friendly and understanding when they may in fact feel frustrated and annoyed. This induces emotional dissonance, which is a discrepancy between the feelings experienced and the feelings displayed (Grandey, 2003). Managing this discrepancy requires emotional labor, which can be stressful. Surface acting is displaying an emotion you don’t actually feel; however, sometimes people get absorbed in the situation and the expression of emotion and actually begin to truly experience that emotion, which is referred to as deep acting and is much less stressful (Grandey, 2003).

Affect and emotion are important in the workplace not only because they are related to job attitudes but because they can affect the climate of the workplace (Zhao, et al., 2007). It is important for today’s organizations to cultivate a climate of cyber awareness and safety; hence it behooves an organization to promote positive affect and emotion regarding cyber behavior.

**Organizational Justice.** Affect is also associated with perceptions of organizational justice. Organizational justice is composed of distributive justice, procedural justice, and interactional justice to create the individual’s overall perceptions of justice (Colquitt et al., 2001). Distributive justice is whether the distribution of rewards is fair. When forming a perception of distributive justice a person will likely view the situation from one of three standpoints: merit, in that whoever works hardest should be best rewarded; need, in that people most in need of reward should receive the greater share; or equality, in that everyone is equally deserving (Greenburg, 1993). Procedural justice is the perception of whether the way the distribution of rewards is decided is fair (Greenburg, 2011). If employees feel their opinions are taken into account when such decisions are made, they are more likely to feel that procedural justice occurred (Brockner et al., 2007). This feeling of being heard is called voice, and it is a very important part of
perceived fairness (Price et al., 2006). Interactional justice, also called interpersonal/informational justice, refers to whether decisions are made with respect and sensitivity (Greenburg, 2011). If employees feel that management is being honest and forthright with them, and that they are being treated politely and with dignity, then they will perceive interactional justice. Employee perception of organizational justice is very important to an organization and has been found to be positively related to satisfaction, commitment, and trust; and negatively related to conflict, turnover intentions, and theft (Cohen-Charash & Spector, 2001; Greenburg, 1993).

Other constructs related to organizational justice that are associated with important organizational outcomes are psychological contract breach and trust (Robinson, 1996). Trust and breach of the psychological contract is an employee’s perception that what was promised or owed them by the employer was not delivered (Robinson, 1996). This is negatively related to performance, satisfaction, and commitment. Psychological contract breach is positively related to intention to turnover, and is also associated with feelings of violation and mistrust (Zhao et al., 2007). While there are many definitions of trust in the organizational context, here trust is considered the intention to accept vulnerability to a trustee based on a positive expectation of their actions (Colquitt et al., 2012). Colquitt, Scott, and LePine (2007) found that some of the precursors of trust are ability, benevolence, integrity, and trust propensity, and that some of the outcomes of trust are task performance, risk-taking, and organizational citizenship behavior. Mistrust is associated with counterproductive work behavior, so it is important to maintain the trust relationship and not to break the psychological contract (Robinson, 1998).

As perception of organizational justice is related to performance, satisfaction, commitment, and trust, it follows that organizational justice might be related to employees’
willingness and desire to comply with cyber safety procedures. If employees feel that they are being treated fairly, they are more likely to respect the rules (Schminke, Arnaud, & Taylor, 2015), which would probably include those regarding cyber behavior.

**Leadership.** Trust in leaders is also an important component of effective organizational behavior (Judge & Piccolo, 2004). Leadership consists of influence, persuasion, and inspiration, which affect follower attitudes, feelings, beliefs, and behaviors (Barling, Weber, & Kelloway, 1996). Effective leadership is a product of the individual and the situation. The leadership process begins with effort exerted by the individual in an attempt to lead, with the hope that this will be rewarded with compliance. In turn, it is expected that compliance will lead to the accomplishment of the organizational goal (Minderovic, 2001). In examining leadership in any given situation, it is important to examine the traits, behaviors, and other characteristics of the leader as well as those of the followers, including their motivation, interpersonal harmony, the number, their cognitive ability, their background and other factors which will not only affect the response of the followers to leadership but which will also influence the behaviors of the leader (Goethals & Sorensen, 2006). Leadership is a function of the traits and behaviors of the leader, the traits and behaviors of the followers, the relationship between the leader and the followers, and the situation, which is made up of the organizational culture, the goals of the organization and the immediate task, as well as the nature of the job itself (Judge, Piccolo, & Kosalka, 2009).

A relationship-based approach to leadership, leadership-member exchange (LMX) has been shown to correlate with important organizational outcomes such as overall job satisfaction, organizational commitment, organizational citizenship behavior, and (negatively) turnover intentions (Ilies, Nahrgang, & Morgeson, 2007). LMX posits that leadership can effectively be viewed as a series of vertical dyadic relationships of two general types: in-group, which is based
on expanded and negotiated role responsibilities, and out-group, which is based on the formal employment contract (Graen & Uhl-Bien, 1995). In-group exchanges are high-quality exchanges with high degrees of mutual trust, obligation, respect, and consideration, while out-group exchanges are of low quality and are characterized by low levels of these properties (Ilies, Nahrgang, & Morgeson, 2007). There are four stages of development of LMX. The first is the vertical dyad linkage, which presents differentiated relationships of leaders with their followers. The second stage of development is leader-member exchange, which shifts the mere description of differentiated relationships into the realm of how these various leader-member exchanges affect organizational outcomes. In the third stage, the process of moving beyond in-groups and out-groups to form high quality relationships between the leader and all followers is ascribed, with this stage referred to as leadership-making. The final stage of LMX is team-making, in which these differentiated dyadic relationships are examined at the systems level perspective. When viewed as a network of interdependencies and relationships, the structure of the leadership becomes apparent (Graen & Uhl-Bien, 1995). The team-making stage of LMX theory is important because it is here where effective leadership behaviors can be identified.

Leadership is a function of the traits and behaviors of the leader and the followers, the relationship between the leader and the followers, and the situation, goals, and tasks (Judge, Piccolo, & Kosalka, 2009). Hence, leadership should play an important role in cyber behavior. Good leadership could greatly influence followers’ willingness and desire to comply with cyber safety measures. In a study with a large sample of employees from a diverse set of organizations in Sweden, transformational leadership was highly related to information security awareness and a strong information security culture (Rocha Flores & Ekstedt, 2016).
Workplace Teams. Work teams display a high level of interaction and work intensively together toward a common goal (Kozlowski & Ilgen, 2006). There is currently an increasing emphasis on teams in the workplace, due primarily to advances in information technology and corresponding increases in specialization and communication (Shen, 2014). A common model for team effectiveness is the Input-Process-Output (IPO) model, in which the organizational context, the task characteristics, and the team composition are some of the input factors, the process factors consist mostly of norms, cohesion, decision-making, communication, and coordination, and the output is the productivity and performance, innovation, and satisfaction of the members (Kozlowski & Ilgen, 2006). More recently, teams researchers have pushed to include the role of time in this process, as well as the consideration of the cyclical nature of the process (Marks, Mathieu, & Zaccaro, 2001). When selecting for maximum team performance, cognitive ability, personality variables, and communication, coordination, and other skills should be considered (Barry & Stewart, 1997). Teams should be trained together in order to create shared mental models, in which the team has a common understanding of the task that is to be performed and of what each individual’s role will be in achieving this goal (Kozlowski & Ilgen, 2006). Teams with higher diversity have a larger pool of knowledge, skills, and abilities, as well as different opinions and perspectives, which enable greater innovation and creativity; however, homogeneity in teams has been linked to lower turnover, greater cohesion, and often leads to higher performance (Marks, Mathieu, & Zaccaro, 2001). Employees working in teams can improve performance but can also lead to negative outcomes. Examples of these include group think, in which a team becomes overly cohesive to the extent to which they become intolerant of “outside” viewpoints; social loafing, which is a tendency of individuals to exert less effort when working in a group than when working alone; and process loss, in which as teams grow larger it
takes more effort to communicate and coordinate efforts (Kozlowski & Ilgen, 2006). Generally, teams should be utilized when a task requires a high level of interaction such that the team approach will simplify the job, and when the task is something an individual is unable to accomplish alone.

The relationship between teams and cybersecurity is bi-directional. As more organizations capitalize on the advantages of cyber teams, cyber safety will become an integral part of the Input-Process-Output model. If measures to protect the safety of the information systems are not taken, the integrity of the team processes and subsequent output could be jeopardized. Just as poor cyber safety could infect the work of the entire team, strong cyber awareness and compliance by one or more team members could help protect the entire team. If just one cyber expert were placed on every team, it is possible a culture of cyber safety could develop within that team through a shared mental model.

**Motivation.** Motivation is important at both the team and the individual level within an organization. Motivation is the combined effects of behavior on three facets: direction, the behavior to be performed; intensity, the level of effort exerted; and persistence, how long the effort is continued (Roskes, 2015). The relationship between motivation and performance is moderated by ability, and is also affected by situational constraints (Shen, 2014). There are many theories of motivation, some of which are intuitively appealing but lack empirical support, others that have some empirical support but limited practical utility, and still others with mixed support. One theory of motivation with both empirical support and practical utility is the Job Characteristics Model (JCM), which espouses that motivation develops through the work itself (Hackman & Oldham, 1976). In the JCM, there are five core job dimensions: skill variety, task identity, task significance, autonomy, and feedback; these lead to the critical psychological states
of experienced meaningfulness of the work, experienced responsibility for the outcomes of the work, and knowledge of the actual results of the work activities. These critical psychological states mediate the relationship between the core job dimensions and personal and work outcomes, which consist of high internal work motivation, high-quality work performance, high satisfaction with the work, and lower absenteeism and turnover (Cleave, 1993). This relationship is moderated by Growth Needs Strength (GNS), which is an individual’s desire to fulfill higher order needs (Hackman & Oldham, 1976).

Goal Setting Theory is another useful model, which asserts that goals work by directing attention toward the goal, increasing effort level, encouraging task persistence, and facilitating strategies to overcome hurdles. Goal Setting Theory assumes the individual has the ability, is committed, and is receiving feedback (Latham, Erez, & Locke, 1988). It is important to be cautious regarding goal setting, as Kanfer and Ackerman (1989) found in a study of air-traffic controllers that setting performance goals while still learning a complex task hindered performance. Winters & Latham (1996) suggest setting learning goals rather than outcome goals in these situations. Research suggests that motivation is linked to personality traits and self-efficacy (Judge & Ilies, 2002), with conscientiousness being most highly associated with goal-setting motivation.

There has been increasing exploration into the motivation behind malfeasant cyber behaviors. Rogers (2006) investigated the typology of hackers, with four motivations emerging—revenge, financial, notoriety, and curiosity, the most common of which is financial. Improving our understanding of what motivates cyber malfeasance would increase our ability to discourage such harmful cyber behaviors. Likewise, learning more about what motivates employees to practice good cyber hygiene would be beneficial in helping us encourage all
employees to be cyber safe. Yet there has been a dearth of research involving what motivates proactive cyber behavior, and more needs to be done. It is vital that organizations understand the motivation behind cyber safety, as its employees are an organization’s best line of defense against cyber threats. Knowledge and training are not necessarily enough, as understanding cybersecurity techniques will not help if an employee is not motivated to utilize them.

Organizational Socialization and Person-Environment Fit. When a new employee begins working at an organization, they go through a period of socialization in which they evolve from being an outsider to becoming an insider (Bauer & Erdogan, 2011). The personal characteristics and the behaviors of the new employee in addition to the efforts of the organization determine how well the employee adjusts, which leads to the employee outcomes (Bauer & Erdogan, 2011). Employee characteristics that can facilitate organizational socialization are extraversion, a proactive personality, openness to experience, and job experience (Bauer et al., 2007). Employee behaviors that help expedite socialization are networking, active information seeking, and active performance feedback seeking (Bauer et al., 2007). Efforts on the part of the organization to assist with the employee’s organizational socialization include formal orientations, realistic job previews, mentors, and socialization tactics dictating roles, norms, and typical sequence of activities (Bauer et al., 2007).

An important factor in how well organizational socialization transpires is person-environment fit. Person-environment fit is what occurs when the characteristics of the employee are well matched and compatible with the properties of the work environment (Kristof-Brown & Guay, 2011). There are different ways in which person-environment fit can occur, including person-vocation, person-job, person-organization, person-group (work team), and person-individual (such as a supervisor or co-worker). Each of these is positively correlated with job
satisfaction and overall performance and negatively related to intent to turnover (Kristof-Brown, Zimmerman, & Johnson, 2005). It is important to select employees that will fit well within the culture and climate of the organization.

It would be beneficial to organizations to include the company’s cyber safety values in the process of new employees’ socialization into the organization. Cyber safety should be an integral part of realistic job previews, formal orientations, and other socialization tactics, and cybersecurity should be stressed by mentors and in feedback provided to a new employee.

**Organizational Culture and Climate.** The culture of an organization is how people perceive the work environment, and the climate of an organization is the way things are done in the organization, with culture being more a property of the subjects, and climate being more a property of the organization (Denison, 1996). Climate consists of environmental feelings and characteristics and perceptions of observable practices, while culture is an historical evolution of shared beliefs over time, consisting of perceptions of values underlying actions (Denison, 1996). Climate is more easily changed while culture tends to be immutable. Despite these differences, climate and culture overlap and complement each other (Denison, 1996). Organizations with strong cultures can be more effective, but there is also evidence that a culture that has been in place for too long can lead to negative outcomes such as group think or overly controlling management (Saffold, 1988).

In a study examining national culture at IBM, Hofstede (1986) found it to consist of five dimensions, including power distance, individualism versus collectivism, masculinity versus femininity, uncertainty avoidance, and long-term versus short-term orientation. Interestingly, these are all dimensions of organizational culture as well. Little research has examined the outcomes of various types of cultures, but it has been found that organizations that place
emphasis on interpersonal relationships as opposed to accomplishment appear to have lower rates of turnover (Sheredan, 1992). Individuals’ perceptions of leader, work group, and organizational climate are strongly related to job satisfaction, job involvement, and organizational commitment (Parker et al., 2003).

Sometimes specific cultures emerge or can be cultivated within organizations, such as a culture of service, diversity, or safety. It would behoove an organization to promote a culture of cyber awareness and safety. Chang and Lin (2015) found that organizational culture significantly influenced information security measures. In another study, it was found that an organization's information security culture is positively associated with employees’ information security awareness, as well as their attitudes toward and beliefs about resisting social engineering (Rocha Flores & Ekstedt, 2016).

**Health and Safety.** Workers who are employed by an organization without a positive safety culture are more likely to take risks than workers in an organization that emphasizes safe work procedures and makes a firm commitment to employee health and safety (Fleming & Buchan, 2002). Garcia, Boix, and Canosa (2004) found that workers complied less frequently with safety rules and exhibited more risky behavior when they rated the safety climate of their organization as low.

The field of Occupational Health Psychology (OHP) is still emerging. OHP is involved in promoting the health, safety, and well-being of workers through the application of psychology (Beus et al., 2010). Some of the dimensions of OHP include job safety to avoid accidents and injuries, psychological oversight to prevent violence and physical and verbal aggression, protection from toxic substances and communicable diseases to avoid illness, and reducing stressors to minimize stress, strain, and exhaustion (Parks & Streelman, 2008). With 40% of
workers reporting that their job is very stressful and work-related stress to U.S. organizations costing $200 billion annually, stress in the workplace is something to take seriously (Nahrgang, Morgeson, & Hoffman, 2011).

Cyber incivility and cyber bullying are health and safety issues that are becoming increasingly problematic in organizations (Giumetti et al., 2011). Using cyber means to attack, threaten, or intimidate an individual is bullying behavior, and it represents a hazard to employees’ emotional and sometimes physical health. Although less severe, cyber incivility through such vehicles as office email can cause an emotional reaction in the recipient due to a rude, aggressive, disrespectful or inappropriate message. Cyber bullying and incivility are likely to undermine performance and production as well as affect the attitudes and emotions experienced by employees who are the victims of such stressors. Furthermore, it is doubtful that cyber awareness and safety would be at the forefront of the minds of employees who are fearful to even open their inboxes.

**Work-Family Conflict and Balance.** Another possible source of stress in the workplace is conflict between work life and home and family life. There can be an issue with people bringing work problems home, bringing home problems to work, a spillover between work and home, and juggling the demands of work and family (Lapierre & Allen, 2006).

There are three types of work-family conflict (WFC): strain-based, where the stress of one spills over into the other; time-based, where there is insufficient time for both or a time conflict; and behavior-based, where work-type behaviors intrude on family life or family-type behaviors are inadvertently exhibited in the workplace, such as treating children like employees or treating employees like your kids (Kelly et al., 2008).
Outcomes of WFC can be dissatisfaction and distress at work and/or at home. It often leads to withdrawal from work and/or family. Job stress, hours spent at work, and job involvement all have a positive relationship with work interfering with family (WIF), while schedule flexibility and work support have a negative correlation (Shockley & Singla, 2011). Marital status, number of children, and family stress are related to family interfering with work (Shockley & Singla, 2011).

Reducing strain of all sorts in the workplace—including physically or psychologically hazardous situations and those evolving from work-family conflict—could have favorable effects on positive cyber behavior. A stressed employee is an employee who is not performing at their best (Arshadi & Damiri, 2013), including in regard to cyber awareness and compliance. Furthermore, with technology increasing the ability for employees to work practically anytime, anyplace, the lines between work and home life can become blurred. Some individuals experience difficulty with boundary management—how and to what degree an employee separates work from home life (Kossek & Lautsch, 2012). Some employees prefer an integrated method in which they may perform work tasks while at home with the family—such as responding to work emails or bringing work projects home—as well as engaging in non-work-related obligations while at work—such as making children’s dentist appointments or shopping for shoes online. Other employees are more segmented and prefer to keep their work life and their home and family life separate. If a segmentor feels pressured to bring work home, it will likely cause strain. There is a different sort of danger regarding the integrator, in that an individual may not feel the impetus to engage in the same level of cyber awareness and safety when working on their laptop at their child’s soccer meet that they would in the office, which could open a doorway to cyber threats.
**Turnover.** Job stress is related to turnover (Arshadi & Damiri, 2013). When an employee voluntarily leaves the employment of an organization, it is referred to as turnover (Campion, 1991). The primary predictors of turnover are job dissatisfaction, ease of movement (other job opportunities), and lack of organizational commitment (Hom, 2011). Attitudinal factors are often involved in turnover, but at times situational factors (such as the birth of a child or the relocation of a spouse) drive the decision (Lee & Mitchel, 1994). There is a small relationship between the performance of the organization and turnover. Individuals with greater organizational commitment, job and community embeddedness, and person-organization and person-community fit are less likely to turnover (Ramesh & Gelfand, 2011).

Generally, turnover is expensive and disruptive to an organization, and it is preferable to keep it low. Turnover requires the selection and training of new employees, as well as their socialization into the organization. A new employee enters a company with no initial awareness of that organization’s cyber safety practices, and until they are brought up to speed could be more likely to be in danger of compromising the organization’s security than a seasoned employee who is better aware. Also, disgruntled ex-employees have been known to engage in cyber malfeasance against their old employers, or even be recruited by outside agents to infiltrate an organization’s information systems (Weimann, 2004). Turnover is not likely a friend to cyber safety.

**Organizational Citizenship Behavior.** Organizational behavior can be positive, negative, or neutral, or anywhere on the continuum. Management assumes the task of attempting to influence employees within the organization to engage in more positive behavior and less negative behavior. Organizational citizenship behavior (OCB) was first conceptualized by Organ (1988) as “individual behavior that is discretionary, not directly or explicitly recognized by the
formal reward system, and that in the aggregate promotes the effective functioning of the organization.” Organizational citizenship behavior is related to contextual performance, which is defined by Borman and Motowidlo (1993) as work behaviors that are non-task related and contribute to the psychological and social well-being of the organization. Both OCB and contextual performance involve behaviors that are beyond the normal requirements of the task, however, contextual performance is rewarded while OCB is not, and while contextual performance is not task-related, it can be role-related (Podsakoff, MacKenzie, Paine, & Bachrach, 2000). Prosocial organizational behavior and extra-role behavior can also be compared to OCB. Prosocial organizational behavior is aimed at helping another individual within the organization, but can be to the benefit of only the individual and not the organization, unlike OCB and contextual performance (Brief & Motowidlo, 1986). Extra-role behavior is very similar to OCB except that it includes actions that are ultimately intended to improve the organization but could have immediate deleterious effects, such as whistle-blowing or protests against perceived problems with the organization, such as social injustice (Organ, Podsakoff, & MacKenzie, 2006). Antecedents of OCB and other related positive work behaviors include job satisfaction, personality characteristics, perceived organizational justice, organizational commitment, task characteristics, and leadership behavior (Organ & Ryan, 1995).

There are many cyber behaviors that may be categorized as OCBs, which will be discussed further on in this paper. Certain proactive cyber behaviors called security assurance behaviors have been found to positively relate to OCB (Dreibelbis, 2016).

**Counterproductive Work Behavior.** In contrast to OCBs, CWBs are negative behaviors, referred to as counterproductive work behaviors (CWB) and defined as behavior that is harmful to the organization or its stockholders (Spector & Fox, 2005). Similar constructs to
CWB are workplace deviance, which is norm-violating workplace behavior; retaliation and workplace revenge, which are harmful behaviors directed at someone who has injured or maltreated them; and workplace aggression, which consists of abusive acts that harm others in an organization (Robinson & Bennet, 1998). Several dimensional models of CWB have been proposed, with dimensions such as lateness and absenteeism, withdrawal, sabotage, bullying, harassment and verbal abuse, and cyber loafing (Spector et al., 2006). Some predictors of CWB include perceived organizational justice, job satisfaction, personality variables, self-control, organizational constraints, and affect (Robinson & Bennet, 1995). An exclusion to CWB is accidental or unintended negative results of behavior, although neglecting or ignoring safety procedures leading up to the accident would be considered CWB.

Certain harmful or dangerous cyber behaviors-- referred to as security damaging behaviors and security risk behaviors-- appear to be strongly related to CWB (Dreibelbis, 2016). In fact, many cyber behaviors could be categorized as CWBs; this relationship will be discussed later in this paper.

**Overall Organizational Behavior.** Organizational behavior is complex. Desired behaviors, such as CWBs, and behaviors that organizations strive to thwart, such as CWBs, stem from the attitudes, affects, and emotions driving employees. An employee’s motivation can be derived from the leadership the employee receives, as well as from the level of organizational justice the employee perceives and how they view the culture and climate of the organization. The attitudes, cognitions, and behaviors of employees shape the way they function within the organization and influence the output of their behaviors. Good person/environment fit through proper selection, along with effective leadership, work/family balance, and attention to health
and safety factors, can foster motivations for behaviors that are in line with desired organizational outcomes.

Organizational behavior is not only more than just one construct, it is also more than simply a sum of concepts. Behavior in organizations consists of vast, interwoven connections of networks that depend upon each other. For example, in order to attempt to understand the type and quality of leadership that exists in an organization, one must examine the culture and climate, the motivational forces present, and the attitudes and affects of the employees. In order to investigate turnover, one must have knowledge of the organizational socialization, the person-environment fit of the individuals, work family conflict and balance, leadership, motivation, perceived organizational justice, and the attitudes regarding health and safety within the organization. When examining what motivates certain behaviors in an organization—such as cyber behaviors-- it is important to consider all aspects of organizational behavior, because each will likely influence the other.

Moving forward to examine organizational behavior in the context of cybersecurity, I will next define what types of threats exist to the safety of information systems. I will then discuss how training occurs in organizations followed by how cyber safety awareness may be addressed through training. Although cyber compliance through training is not the subject of this study, training is one of the most widely-used methods of controlling security and merits thorough discussion. Some of the most prevalent cyber training delivery methods and the advantages and disadvantages of each will also be addressed in this section.

Following this, I will discuss attitudes and the routes through which attitudes and motivations can be changed. Employees’ attitudes toward cyber security and motivations to be safety conscious and compliant can stem from many sources. I will introduce the construct locus
of control and explain why I think it is one of the sources contributing to a person’s cyber behavior. In addition, I will discuss risk perception and the part I believe it will play in the relationship between locus of control and cyber misbehavior.

After discussing the relationships the literature supports, I propose my hypotheses and submit the models representing them. After that I investigate another area of interest regarding the relationship between risk perception and sensation seeking, and propose research questions in respect to these constructs. The relationship between these constructs in regard to their relationship with cyber behaviors is yet unexplored, so with no direct theoretical support to serve as a guide these investigations will be posed as research questions rather than hypotheses.

Cyber-Threats Defined

Before investigating what constitutes negative cyber behavior, it is important to determine what cyber-threats exist. Cyber-threats are many and varied (Kirwan & Power, 2011). A computer user can permit any number of hazardous outside attacks simply by opening an email from an unknown source. For instance, an employee might receive an email from a cyber-criminal saying that the employee’s company email account is outdated and nearing capacity and must be updated or it will be deleted, with a link to click to update the account. If the employee clicks that link it allows the cyber-criminal access to the organization’s computer system. Convincing a computer user to give up information or commit an action they would not have otherwise done is referred to as social engineering, which is also known as human hacking or simply hacking (Conheady, 2014). Phishing is a type of online social engineering in which the criminals use increasingly sophisticated techniques of persuading people to surrender personal information (Dodge, 2007). Reverse social engineering is also becoming more commonplace, usually consisting of the attacker disabling the system and then posing as a technician to “help”
the user. In this way, the user generally has significantly more trust in the attacker and is more likely to give up passwords and sensitive information. Once they have gained access to an organization’s computer system, cyber-criminals can install malicious software called malware on the computer that can destroy systems or render them inoperable, or the malware can corrupt, destroy or steal data (Leach, 2015). Employees tend not to be as cognizant of security risks while engaging in seemingly friendly activities such as blogging, instant messaging, and social computing (Islam & Abawajy, 2013). The behavior of the computer users is the most vital antecedent to most cyber attacks. The majority of cyber-criminals depend on the user to behave in such a way that allows the criminal entry to the system.

Training in Organizations

Most organizations employ training to facilitate the practices they want to encourage in their employees and to discourage the practices they want to avoid, as well as to confer new information and teach new procedures. Job training refers to the planned and purposeful endeavor on the part of an organization to facilitate employees’ acquisition of job-related knowledge, skills, competencies and behaviors (Noe, Tews, & Marand, 2013). Kirkpatrick’s hierarchical model of training outcomes is usually utilized to assess the effectiveness of training programs. This model consists of four levels of training effects, including the reactions of the trainees to the process and content of the training, the skills acquired and the knowledge learned, the change in behavior after the training, and individual and organizational outcomes and improvements (Noe, Tews, & Marand, 2013). Job training can be instrumental in fostering motivation and in forming employee attitudes (Schmidt, 2007), and often provides a sense of success and progression through the continual learning of the employee (Huang & Su, 2016).
Deterring Cyber Misbehaviors Through Training

Albrehtsen and Hovden (2010) assert that the most cost-effective method of controlling security is training employees in security awareness. Shaw, Chen, Harris, and Huang (2009) define security awareness as the level of a computer user’s understanding of the importance of information security and of their role in exercising sufficient levels of information security control that will protect the system’s data and networks. With proper awareness of appropriate security measures, employees can become a company’s most effective line of defense against cyber-crime (Kumaraguru et al., 2007). There are many methods by which to raise awareness of cybersecurity issues, such as posters, emails, pamphlets, screensavers, videos, newsletters, training sessions, meetings and gaming. Both the information conveyed and the method of delivery is important, and it is necessary to relay the information in several different ways so the user is sure to receive the message (Shaw et al., 2009). In order to facilitate awareness of changes and updates and keep security measures salient it is also important that a security awareness program be ongoing and become an intrinsic part of the organizational culture (Kruger & Kearney, 2006).

According to Shaw et al. (2009), an effective security awareness program approaches awareness through three steps. The first step is perception, or gaining an awareness that a threat exists. Once employees become aware of the presence of security risks, the second step is comprehension, which is the ability to understand, comprehend, and assess the threats that may be present in different situations and how to combat them. The third level in improving security awareness is projection, which is the ability to anticipate potential security risks, much in the way a skilled expert such as a surgeon or air traffic controller anticipates future conditions. It is preferable to prevent security issues than to rectify cybersecurity mishaps (Shaw et al. 2009).
Security awareness exists along a continuum, with some users not yet at the perception stage—unaware of the dangers—and others are at the far end of the projection level, with many of these individuals responsible for creating the firewalls and other preventive measures the rest of us depend on. The goal of a security awareness program is to shift the employees as far along this continuum as possible.

**Training Delivery Methods**

Paper-based security awareness delivery methods such as posters, pamphlets, and newsletters are common in organizations. If placed strategically, posters have the advantage of being accessible by many people, but the downfall is that they usually only address one simple topic and are often overlooked or become ignored (Abawajy, 2014). Newsletters and pamphlets have the advantage of being able to convey many messages at once, but they depend on proper distribution, may not appeal to everyone, and there is no way of ensuring the employees read them (Wilson & Hash, 2003).

Instructor-led security awareness methods overcome some of the shortfalls of paper-based delivery, but they are not without disadvantages of their own. Although many people claim to prefer this method, many others find it boring; additionally, changes in security issues can’t continually be addressed without holding classes on a regular basis, and it’s expensive (Abawajy, 2014). If entirely instructor-led this method also doesn’t require the listener to think logically or reflect on personal application. This can be overcome by conducting facilitated group discussions based on sharing knowledge and experiences (Albrechtsen & Hovden, 2010).

There are numerous online security awareness delivery methods. Emails are quick, easy, cheap, and flexible, but also time-sensitive and may be ignored (Wilson & Hash, 2003). Web-based computer security awareness training (WBT) is flexible, self-paced, and user-friendly
There are also many blogs and tutorials devoted to computer security awareness. Shaw et al. (2009) found that media methods higher in information richness produced greater security awareness results. Richness can be determined by capacity for immediate feedback, the number of cues and channels available, the variety of the language, and the extent to which intent is focused on the participant (Shaw et al., 2009). To this effect, e-learning programs would not be as informationally rich as multimedia, which combine text, sound, image, animation, music, and video and virtual reality. Yet multimedia is only accessed linearly, so it is not as rich as hypermedia, which contain hyperlinks and does not necessitate a sequential process (Shaw et al., 2009). While Shaw et al. (2009) found that hypermedia is most effective in promoting security awareness, they did note that human interaction is the richest medium of all.

Of course, the richness of the delivery method is irrelevant if the employee does not engage in the media program. Cone et al. (2007) assert that Web-based delivery methods face the challenges of ensuring that users devote appropriate time and thought into the process and that the method challenges the users and does not become monotonous, with a major短coming of the method being that it provides no avenue for dialogue or discourse for further elaboration. Game-based delivery methods can be more engaging to many users, with their high levels of interactivity and challenge often more motivating than Web-based programs. A game-based delivery method called Anti-Phishing Phil, which is designed to teach users to distinguish between legitimate URLs and phishing ones, was found to have a better result than other methods intended to accomplish the same task (Sheng et al., 2010). Videos can be a cost-effective delivery method with both visual and audio learning that can be independently paced so the user can stop when tired or bored (Abawajy, 2014). Videos can also be used repeatedly, which is an economically sound way to remind employees of security awareness, although
videos should be updated periodically to reflect changes in security measures and to prevent employees from becoming bored with them. Interactive videos can be more engaging than standard videos but cost more.

**Attitude Change**

In order for any training method to effectively change employees’ behaviors, it must first change their attitudes. Attitude is an individual’s evaluation of an object, thought, concept, or person (including oneself) (Albarracin, Wallace, Hart, & Brown, 2012). An individual’s attitude toward something can be positive, in which case they will favor and support such an item or construct, or negative, in which case they will avoid, blame, or intend harm towards the item or construct, or it may be neutral in that the item or construct will not elicit much of an attitude at all (Petty & Briñol, 2015). Attitudes form as evaluative responses to experiences or observations, and once they are established they tend to prevent additional evaluation of subsequent experiences of a similar nature (Eagly & Chaiken, 1984). Evaluative responses resulting in attitude formation can be cognitive, affective, or behavioral, and can be either overt or covert (Eagly & Chaiken, 1984). Attitudes can also arise from exposure to the attitudes of others whom the individual holds in high regard or with whom the individual wants to feel a sense of belonging. The people or groups with whom an individual wants to belong are often referred to as a reference group in regard to that individual (Albarracin et al., 2012). Attitudes are not stable, and can change through social influence and through a person’s need for their attitudes to match their behavior.

Attitude has been found to influence behavior through its impact on an extensive range of cognitive processes, such as perception and interpretation, reasoning, and social inference. (Eagley & Chaiken, 1984). Strong, highly accessible attitudes are more likely to shape an
individual’s behaviors and cognitions in a manner reflective of the attitude (Bargh et al, 1992). People have a need for their behavior to be in concordance with their cognitions, otherwise it creates a condition called cognitive dissonance where one’s beliefs are in conflict with one’s actions (Eagley & Chaiken, 1984). Cognitive dissonance usually results in either a behavior change, a cognition change, or more likely an added cognition that somehow rectifies the discordance between the dissonant behavior and cognition (Eagley & Chaiken, 1984). When a person experiences conflicted evaluations of an element—in that there are both positive and negative responses—an ambivalent attitude usually arises (Thompsen & Zanna, 2005). In addition to attitude shaping behavior, behavior can also shape attitude. Proposed by Bem (1967), self-perception theory asserts that when attitudes, emotions, or other internal states are weak or ambiguous, these states might be inferred from knowledge of the circumstances or the behavior. In this case the individual is responding to her own cues in the same way that an outsider might. If someone observes his neighbor doing a lot of walking, he might assume she enjoys fresh air and exercise; likewise, the neighbor herself may adopt the attitude that she enjoys fresh air and exercise from the fact that she walks a lot.

If an individual holds the cognition that information security is very important, yet they keep their password on a sticky note in their desk drawer, their beliefs and their behaviors are in conflict, creating cognitive dissonance. This might create the need for an additional cognition, such as the belief that their time is so valuable that it is better served in ways other than memorizing or safely storing passwords, or this cognitive dissonance might result in a behavior change, such as memorizing the password and destroying the sticky note. If an organization can change employees’ beliefs and cognitions, they can potentially influence behaviors. Attitude
change mediates the relationship between belief/cognition change and behavior change (Petty & Briñol, 2015) and therefore is very important.

**Influencing Cybersecurity Attitudes**

It has been suggested that there are two routes to persuasion, the peripheral route and the central route (Petty & Weggener, 1998). Persuasion through the peripheral route is not based as much on the quality of the argument as it is on the credibility of the source or the number of people espousing it, or other such heuristics (Petty & Weggener, 1998). Persuasion through the central route requires the person to be motivated to consider the argument and to be able to devote the time and attention to the argument. In this process, the person is more likely to consider the content of the information presented and deliberate on the quality of the argument (Petty & Weggener, 1998).

There are many practical applications of attitude change and persuasion theory in the workplace. Self-generated persuasion is a technique by which a person is encouraged to find arguments to support a position, after which they will generally be much more in support of the position themselves (Eagley & Chaiken, 2007). An organization could ask employees to develop some arguments for why cybersecurity awareness is so important, ostensibly to use in training and awareness sessions, which would very likely result in those employees holding information security in higher regard. This stems from cognitive dissonance theory; if a person has a lot of reasons why information security is important then they will probably believe that they must think it’s important.

Another persuasion technique that uses cognitive dissonance theory is the foot-in-the-door technique, where a small concession is asked of someone, with the idea that they will later give in to greater demands, as they feel that they must support this issue if they agreed to the
smaller request (Petty & Weggener, 1998). For example, if everyone in the office is asked to sign a pledge supporting greater information security awareness in the workplace, this seems like a small thing to do and most would probably be willing to do it. If in the following week the employees who signed the pledge are asked to participate in a voluntary information security awareness class, they would be much more likely to do so because they have already signed a pledge stating that this is important, therefore they will believe that they must think it is important.

**Locus of Control**

Behavior in the workplace can be seen as a consequence of the employee’s attitudes towards different job-related targets, and also of the employee’s dispositional profile and current context. An attitude is an evaluation of a situation or an object, which has a cognitive and an evaluative component, as well as an intention aspect. A trait is an individual disposition, which while not immutable tends to remain stable over time. Locus of control is a trait.

Locus of control comes from social learning theory and refers to the extent to which a person believes the environment is controllable and responsive (Rotter, 1966). This perception of control derives from expectations that are shaped internally by the individual’s own efforts or externally by environmental factors beyond the control of the individual. Those with internal locus of control believe that they can influence what happens to them, that they have personal agency over gaining rewards for their actions. Those with external locus of control believe their environment is uncontrollable and that they have no influence over whether or not they gain rewards. Locus of control differs from self-esteem and generalized self-efficacy in that locus of control involves beliefs about the environment (and its controllability) rather than beliefs about the self (and one’s worth and capabilities) (Johnson, Rosen, Chang, & Lin, 2015). While high
self-esteem would be considered advantageous to most people, the desirability of internal locus of control depends on the situation. It would not be advantageous to a person’s self-evaluation to experience negative outcomes when they believe they are in control of the environment, whereas a person with external locus of control will not think less of themselves when rewards do not come their way because they do not believe their actions have anything to do with it (Weiner, 1985).

These beliefs are generally not contextual and tend to be broad in scope, affecting people’s feelings, thoughts, and behaviors (Spector, 1986). Although it is sometimes disputed that LOC is a personality construct (Stewart, 2006), and it is suggested by You, Ji, and Han (2013) that the internality-externality dimension of LOC may be confused with the personality construct of introversion-extraversion, Rotter’s (1966) contention was that people would generally trend in one direction or another (Turnipseed, 2014). While LOC can vary based on environmental factors, LOC is a dispositional trait rather than a situational state (Wallston, 1992). LOC scales are often dichotomized into external LOC and internal LOC, in order to create a between-participants variable, and this is a poor practice that has contributed to the false assumption that LOC is more stable than it is (Lefcourt, 1982), however, Rotter’s I-E scale was designed to measure general LOC across a broad spectrum of situations, rather than any specific context. Since Rotter’s (1966) development of his LOC scale, many context-specific measures have been developed, such as a LOC scale for pilot safety (Hunter, 2002), one for sales (Chung & Ding, 2002), drinking (Donovan & O’Leary, 1978), academic success (Trice, 1985), and well over a dozen more. Turnipseed (2014) questions the value and contribution of these myriad specific measures, as well as their psychometric legitimacy. While it might prove advantageous to utilize a few contextually-specific LOC scales, such as in the areas of work and health, theory
and practice demonstrate the efficacy and sufficiency of the general LOC scale in the vast majority of situations (Turnipseed, 2014).

Aside from the areas in which a specific LOC scale has been developed, LOC has been used in many settings such as education, safety, medicine, construction, and work. Internal LOC has been found to be associated with a more favorable attitude toward computers (Coovert & Goldstein, 1980). In a study of cyberloafing, external LOC was found to be related to greater involvement in the more dangerous types of cyberloafing—deemed serious cyberloafing—such as online gambling, accessing pornographic sites, illegally downloading music, or other activities that either consume a large amount of the employee’s time or expose the organization to legal liabilities (Blanchard & Henle, 2008). Interestingly, there was no relationship between LOC and what Blanchard & Henle (2008) call minor cyberloafing behaviors, such as browsing news headlines or sending and receiving personal email, indicating that individuals high in internal locus of control have little problem with engaging in petty cyber misbehaviors at work but steer clear of the more dangerous activity. In studies of forestry and construction workers, it was found that external LOC is associated with more risk-taking than internal LOC (Salminen, Klen, & Ojanin, 1999). Research shows that people higher in internal LOC are more likely to use sunscreen (He, 2014). Wichman and Ball (1983) found that those high in internal LOC were more likely to have stronger self-serving biases, illustrated in a study of pilots in which internal LOC was related to the perception of skill and the perceived unlikelihood of having an accident. In another study, it was found that internal LOC drivers were less likely to have vehicular accidents (Arthur, Barret, & Alexander, 1991). Airplane pilots tend to exhibit more internal LOC than external, and internal LOC in pilots is related to the experience of fewer hazardous events (Hunter, 2002). In another study of airplane pilots, internal LOC was found to have a direct
effect on pilot safety operation behavior (You, Ji, & Han, 2013). Piloting an aircraft often requires decision-making in situations where the consequences of unsafe actions can be dire. While poor cyber safety behaviors are not usually life-threatening, they can be devastatingly costly in other ways. As LOC has been demonstrated to predict behavior in critical situations, I hypothesize that this will generalize to cybersecurity behaviors.

Hypothesis 1: Higher internal locus of control will be associated with a lower level of cyber misbehaviors, while lower internal locus of control will be associated with a higher level of cyber misbehaviors.

Figure 1. Model 1: Locus of Control Associated with Cyber Misbehavior

Risk and Risk Perception

Before an individual can form an intention to utilize a protective action, there must be the perception of risk. The National Safety Council (2003) defines risk as “a measure of the probability and severity of adverse effects.” This is a qualitative calculation of how likely a negative incident is to result from a set of actions, as well as assessing how unfavorable the consequences would be if the incident were to occur. This assessment depends upon a person’s risk perception and risk tolerance.

Risk perception is an individual’s ability to determine the level of risk, and risk tolerance refers to their willingness to accept a certain degree of risk (Weinstein, 1984). There are macro-level factors that influence risk perception and tolerance, such as organizational culture and climate, organizational trust, and enforcement (Fleming & Buchan, 2002). These are institutional
or functional factors. Meso-level factors occur at a community or peer-to-peer level, and consist of elements such as peer pressure and conformity (Allen & Brown, 2008). Factors that influence risk perception and risk tolerance at the micro-level are of an individual psychological nature, such as an individual’s perceived knowledge regarding the risky situation, their feeling of personal control, and optimism bias (Huang et al., 2007). Optimism bias is a person’s inclination to believe that a negative event is less likely to happen to them than to other people, or the perception that they are more able than others to contend with a negative event should one occur (Weinstein, 1984).

Risk perceptions can be deliberative, affective, or experiential. Deliberative risk perceptions pertain to logical, rule-based assessments (Tversky & Kahneman, 1983), perhaps regarding how likely an email from an unknown source is to contain malicious material. In this case, the individual makes a rational, cognitive, reason-based judgment of the expected utility of opening the email in relation to the likelihood of a negative consequence occurring (von Neumann & Morgenstern, 1947). In contrast, affective risk perceptions are driven not by dispassionate deliberation but by an emotional response to a threat (Dillard, Ferrer, Ubel, & Fagerlin, 2012). Affect and emotion are critical elements in any decision-making involving risk (Lowenstein, Weber, Hsee, & Welch, 2001). Affective risk perceptions have been found to predict many health and safety behaviors, perhaps more than deliberative risk (Ferrer et al., 2016). Experiential risk perceptions are not rational, reason-based judgments nor are they entirely affective responses. Instead, experiential risk perceptions are outcomes of heuristic decision-making rules based on learned associations (Epstein, Pacini, Denes-Raj, & Heier, 1996). This type of risk assessment occurs very quickly.
Theories Related to Risk Perception and Risk Tolerance

**Protection Motivation Theory.** One of the most cited theories regarding risk perception and risk tolerance is protection motivation theory (PMT). PMT explains how people cope with threats, asserting that people are more likely to seek protection from threats if they perceive themselves as vulnerable, they believe the consequences would be serious, they think the suggested course of action will effectively obviate the problem, and they feel they have the ability to execute the preventative measures (Rogers, 1975). Perceived vulnerability (PV) is an individual’s judgment of how likely the threat is to occur, such as the probability of a security breach. Perceived severity (PS) is the individual’s assessment of the potential severity of the repercussions, such as the ramifications of a security breach. The threat appraisal process is a combination of perceived vulnerability and perceived severity. A person’s perception of their ability to contend with the potential fallout should the threat occur is referred to as coping appraisal (Rogers, 1975). Coping ability is the sum of the individual’s response efficacy plus their self-efficacy, minus the response costs. Response efficacy (RE) refers to the perceived efficacy of the suggested behavior in combatting or preventing harm, such as the user’s judgment of the effectiveness of information security protection software. Self-efficacy (SE) is the user’s belief that they are capable of performing the recommended action, such as properly utilizing the information security methods. Response costs (RC) consist of the costs of engaging in the proscribed behavior, such as the effort and the time involved (Plotnikoff & Trinh, 2010). Therefore a fear appeal message directed at nurses that they should not leave the computers open at the nurses stations might be effective if: the nurses believe that the practice is dangerous in that patients’ personal information could be compromised; the results of leaving a computer open might affect them, possibly by getting them reprimanded or fired; that utilizing a strong
password, not sharing it, and changing it often would effectively keep unauthorized users out of
the information system; and that they are capable of choosing an adequate password,
remembering it, and keeping it to themselves.

Protection motivation theory appears to be linked to the dual-process models of
persuasion (Anderson & Agarwal, 2010). Gleicher and Petty (1992) found that when participants
were exposed to a message about campus crime, they carefully processed it if it reassured them
about the problem, but they only superficially processed it if their fear had already been assuaged
and the message might only cause renewed doubt. Additionally, this same processing pattern
regarding the campus crime message occurred when fear was aroused using an unrelated topic,
illustrating that fear may arouse a general protection motivation, which may affect all safety-
oriented message processing (Gleicher & Petty, 1992).

Situated Rationality Theory. The argument exists that it cannot be assumed that risky
behaviors are inherently irrational. Situated rationality theory posits that if the reward for a given
risk is great enough, it can then be considered rational to take this risk (Keating & Halpern-Felsher, 2008). Often the production-focused structure of business appears to reward unsafe
practices in terms of gains in output, compensation, and recognition. If an employee is going to
enjoy increased productivity and its associated payoff as a result of engaging in some risky
behavior, this cannot be viewed as irrational. Many seemingly irrational behaviors may have a
reward for the individual committing them that to them is worth the risk. The greater the benefit
perceived, the less risk will be perceived (Finucane et al., 2000). If sharing files with an
unauthorized coworker enables an employee to get a task done faster and complete a project on
time, the reward may lessen the perception of risk.
**Risk Compensation Theory.** Also called risk homeostasis theory, risk compensation theory states that individuals will adjust their risk-taking behavior in accordance with their feeling of security. In effect, people will engage in more risky behavior if they believe adequate safety measures are in place. Much of the research in risk compensation theory is in the area of transportation, and results are mixed. Studies show that anti-lock brakes caused people to shorten their following distance and increase their speed (Aschenbrenner & Biehl, 1991; Janssen, 1994). However, some researchers argue that people do not have the ability or the attention to adjust their actions in accordance with perceived safety measures (Robertson & Pless, 2002). A study found that the decrease in traffic fatalities between 1964 and 1990 was 90% due to laws regarding drunk driving and seat belt wearing, which indicates that people did not adjust their risk levels under presumably safer conditions (Robertson, 1998). However, another study found that children who were given a helmet and wrist guards to wear while navigating an obstacle course ran the course more recklessly—and tripped and fell more—than those who were not given protection (Morrangiello et al., 2007). Additionally, when loggers were given protective gear, they anticipated fewer threats, became more careless, and increased their speed (Klen, 1997), and workers wearing an abdominal belt estimated a higher safe lift weight than those without a belt (Bridger & Freidberg, 1999). It might be prudent not to overplay the efficacy of information security features in place in organizations at the risk that they may create a false sense of security in employees.

**Social Control Theory.** Some research shows that a greater affiliation with and connection to a person’s workplace reduces their likelihood of engaging in risky behavior, in that behavior conformity is increased by connectedness to an organization (Hirschi, 1969). Employees who identify strongly with their organization are more likely to follow safety
procedures, encourage their coworkers to follow safety procedures, and to report safety violations of others (Ford & Tetrick, 2011). Participation in hazard-identification programs has been shown to increase employees’ affiliation with the organization and increase safe practices (Clark & Ward, 2006).

**Social Action Theory.** The premise behind social action theory is that individuals tend to conform to the norms of the group in order to avoid sanctions (Cooper, 2003). Therefore, propensity toward risk can be related to group members’ expectations. This can be beneficial in an organization with a culture of safety, in that these employees will tend to have a more positive view of safety procedures and be more likely to engage in safe behavior (Mullen, 2004), but in a culture where risky behavior is prevalent it is likely that newcomers will adopt the same attitude toward safety.

Social action theory and social control theory can be viewed as macro-level theories in that the impetus for risk arises at the institutional level. Situated rational theory is at the meso-level, in between organizational and individual. Protection motivation theory and risk compensation theory are at the micro-level, as they relate to risk perception from an individual perspective. These theories are not entirely disparate, and all have their merits. When designing and implementing cyber safety awareness programs, it would be wise to implement elements from all levels from which risk perception and risk tolerance can arise.

While the literature regarding risk can be applied to risky cyber behavior, cybersecurity risks are specifically defined as operational risks to technology and information assets that have repercussions regarding the integrity, availability, or confidentiality of information or information systems (Cebula & Young, 2010). It is critical to organizations’ well-being that employees exercise behaviors that minimize cybersecurity risks.
Clearly, risk is a complex construct. There are many factors involved in how and when individuals will perceive risk, how much risk they will perceive, and what their course of action will be in a situation perceived as risky. Many situational factors are involved, so there can be no one formula for the process of the perception of risk and the expected response. Often an individual will engage in a behavior they perceive as risky if the potential gain is high enough. In this vein an employee may share passcodes to sensitive information with fellow employees who are not cleared at his level of security even if he recognizes this as risky, because allowing his co-workers to access the information without going through him every time saves him time and effort. Other times, an employee may perceive less risk if she feels safeguards have been put in place, even if those safeguards are there because the situation is a very risky one. A government agent may open an email from an unknown source because she knows that the agency has the best security money can buy, so she perceives less risk. Despite the fact that these types of behavior occur every day, along with myriad other very different types of risk assessment/perception/response behaviors, it can still be said that in general, it can be expected that a higher perception of risk in a situation will likely be associated with less engagement in that risky behavior. If an employee thinks certain cyber behaviors are risky, they would probably be less likely to commit them.

**Cyber-Behaviors Defined**

The National Security Institute (2009) asserts that most cyber incidents occur “not because technology has failed to deliver but because of human failure.” The proportion of inside security breaches appears to be on the rise: the Computer Security Institute reported that about half of security breaches originated from inside the organization in 2004 (Gordon & Richardson, 2004), while the National Security Institute (2009) reported this proportion to be at 75% in 2009.
The IBM Security Services 2014 Cyber Security Intelligence Index (2014) found that inside
error was at the root of over 95% of the security incidents at IBM in 2013. It is clear that the
behaviors of the computer users are the greatest threat to organizations.

Several taxonomies exist regarding cybersecurity errors. Taxonomy focuses on
classification, which separates information by type. Unlike nomological science which revolves
around uniformity; taxonomy delves into the diverse, focusing on what makes things different
(Im & Baskerville, 2005). The existing taxonomies of errors stem from Norman’s (1981)
taxonomy of error, consisting of mistakes, which are actions that prove to be inappropriate, and
slips, which are actions that are not what was intended. Kraemer and Carayon (2007) later added
violations, defined as committing unsafe acts.

Loch, Carr, and Warkentin (1992) developed a taxonomy for information systems
security errors which is composed of four dimensions: non-human external error, human external
error, non-human internal error, and human internal error. The human error was then further
divided into intentional and non-intentional error, with the consequences divided into
information disclosed, data modified, data destroyed, or denial of use.

Stanton, Stam, Mastrangelo, and Jolton (2005) developed a six-element taxonomy of end
user security behaviors that vary along two dimensions. The first dimension is user expertise,
which involves the technical knowledge and expertise of the user, which can be high or low, and
the second factor is user intentions, which pertains to where along a spectrum from malicious to
neutral to beneficial the user’s actions fall. Therefore, an individual with high expertise and
malicious intentions would fall under the category of action called intentional destruction, one
with low expertise and malicious intentions would be under detrimental misuse, one with high
expertise and neutral intentions would fall under dangerous tinkering, a person with low
expertise and neutral intentions would be in the category of naïve mistakes, an employee with high expertise and beneficial intentions would exhibit aware assurance, and someone with low expertise and beneficial intentions would be classified under basic hygiene (Stanton et al., 2005).

Yet another avenue for classifying security threats is Im and Baskerville’s (2005) Information Systems (IS) threat taxonomy. In this approach, threats are seen as accidental or deliberate, with accidental threats further broken down into human errors and catastrophes, and deliberate threats broken down into mode and motive. There are four possible modes of deliberate threat, referring to the individual’s method of attack: physical assault, falsification, malicious code, and cracking of the infrastructure. Motive of a deliberate threat can consist of fraud, vandalism, or espionage (Im & Baskerville, 2005).

In their taxonomy of cybersecurity risk, Cebula and Young (2010) divide risk into four classes: actions of people, system and technology failures, failed internal processes, and external events. Risks related to the actions of people consist of any “action, or lack of action, taken by people either deliberately or accidentally that impact cyber security” (Cebula & Young, 2010). This is further divided into three subclasses: inadvertent, deliberate, and inaction. The inadvertent subclass consists of three elements: mistakes, which are accidental incorrect actions taken by an individual who was aware of the correct procedure; errors, defined as incorrect actions taken by an individual who did not know the correct procedure; and omissions, which consist of an individual failing to take a known correct action, often a result of rushing through a task. Deliberate risks are actions that are intentionally taken to do harm, and consist of fraud, an action deliberately taken to benefit oneself at the expense of the organization; sabotage, a deliberate action take with the intent to cause a failure in an organizational process or asset; theft, the taking of organizational assets intentionally and unauthorized; and vandalism, deliberately
damaging organizational assets, often randomly. The final subclass of cybersecurity risk regarding the actions of people is inaction, which is broken into skills, referring to a failure to take necessary action due to a lack of ability; knowledge, failing to take appropriate actions as a result of ignorance; guidance, which describes an individual who is knowledgeable but lacks the necessary guidance or direction; and availability, which occurs when a resource necessary to carry out the task is unavailable or nonexistent (Cebula & Young, 2010).

Guo (2013) examined the previously discussed taxonomies and concluded that the following dimensions emerge as those associated with the security threat of organizations’ information systems: intentionality, which refers to whether the behavior of the employee was intended or unintended; motive, whether or not there was malice behind the behavior; and expertise, meaning the level of information systems skill and knowledge necessary to commit a certain behavior. Guo (2013) added the following dimensions to the taxonomy: job relatedness, defined as the extent to which the behavior is related to the employee’s job; consequence, which refers to whether the behavior causes damage or is likely to cause damage; action vs. inaction, which indicates whether the behavior was active or passive, such as sharing a password vs. neglecting to change a password; and rule, which denotes whether the behavior breaks a rule or a law, whether it is an organizational rule or a state or federal law. With these behavioral dimensions in mind, Guo (2013) proposed a re-conceptualization of the taxonomy of security related behavior in the workplace. Guo (2013) divides the behaviors into four broad classifications: security assurance behavior (SAB), which is active, protective behavior; security compliant behavior (SCB), which consists of behaviors that are in line with organizational policy; security risk-taking behavior (SRB), which is made up of behaviors that are risky to the organization; and security damaging behavior (SDB), which refers to behavior that will damage
the organization’s information systems. Each of these categories has an intentionality, motive, expertise, role, job relatedness, consequence, action vs. inaction, and rule designation, as well as other associated characteristics.

In categorizing the positive cyber behaviors as defined by Guo (2013), the cybersecurity equivalent of OCB might be security assurance behavior (SAB), defined by Guo (2013) as active, effortful behaviors by an individual in an organization with the purpose of protecting the information systems of the organization. Security assurance behaviors have been found to be positively related to OCB (Dreibelbis, 2016). Just as much of the behavior in organizations will likely be neutral in nature—not harmful but not beyond expectations either, just the normal task performance that is in the job description, it is to be expected that most cyber behaviors would fall under this category also. These neutral behaviors in cyber terms would be the security compliance behaviors, defined by Guo (2013) as behaviors and actions that comply with and are in line with the security expectations and policies of the organization. While these behaviors prevent harm from befalling the organization, there is no intention on the part of the employee to actively protect the organization. CWB in cyber terms would likely be referred to as security damaging behaviors (SDBs), which are defined as behaviors that are directly damaging to an organization’s information system and are in violation of company policy (Guo, 2013), and in fact both security damaging behaviors and security risk behaviors prove to be strongly related to CWB (Dreibelbis, 2016). However, an exclusion to CWB would be accidental or unintended negative results of behavior, although neglecting or ignoring safety procedures leading up to the accident would be considered CWB. Therefore Guo’s (2013) fourth category of information security related behavior, security risk behaviors (SRBs), would also be deemed a CWB, but the negative results of the action—if any—would not be. Guo (2013) defines SRB as behaviors that
put the organization’s information security systems at risk but without the intention of causing harm. An SRB would be a CWB but any deleterious effects of the behavior would not be because they would be considered an accidental result of the security risk behavior.

**Risk Through Misbehavior**

The focus of this study is on Loch et al.’s (1992) nonintentional human error, Stanton et al.’s (2005) naïve mistakes, Im and Baskerville’s (2005) human errors, Cebula and Young’s (2010) inadvertent actions, and Guo’s (2013) security risk-taking behavior. These are all behaviors that pose a risk to the organization, but that risk may not be clear or imminent and the employee committing the behavior has no purposeful intention of damaging the organization’s information system. Often these risky behaviors occur through simple negligence (Herath & Rao, 2009). Crossler et al (2012) term these unintentional cyber risky behaviors “misbehaviors.” There are numerous risky misbehaviors that employees can pose through negligence, such as failing to update or protect computer passwords or choosing weak passwords, neglecting to run recommended updates, opening suspicious email attachments without checking for viruses, or leaving a computer unlocked and unprotected (Hu et al., 2012). An employee visiting an unauthorized website could allow the installation of malware on a work computer without even realizing it (Markoff, 2010). According to Schmidt (2012), a study conducted by the Department of Homeland Security discovered that when they placed USB drives on the ground in the parking lot, 60% of employees picked them up and plugged them into company computers, with that percentage going up to 90% when the USB was imprinted with the operation’s logo. Most organizations prohibit the use of private USB drives in company computers and this type of noncompliance could be disastrous, installing malicious software onto a company computer
through which an outside party could collect and transfer sensitive information, all through no ill intentions of the employee committing the act (Mills, 2010).

Risk assessment essentially obviates or streamlines more complex cognitive demands (You, Ji, & Han, 2013). Risk assessment requires a realistic appraisal of one’s own capabilities as well as an accurate assessment of external factors in order to ascertain the risk involved in the situation; it is a cognitive process in which either overestimating one’s abilities or underestimating the situation may lead to a misjudgment of the risk (Hunter, 2002; You, Ji, & Han, 2013). When occupied with work tasks, an employee must make quick assessments regarding what behaviors will be most expedient and productive while keeping risk at an acceptable level. Cyber misbehaviors may be deemed acceptable if the payoff is high and the risk is assessed as low, such as giving an unauthorized coworker access to a file so they can help you meet a work deadline (Farahmand, Atallah, & Konsynski, 2008). In a study of airline pilots, Hunter (2002) found that pilots who rate scenarios on the Risk Self-Perception Scale as lower in risk were involved in more hazardous events. Entrepreneurs who rate risk as low are more likely to start a business venture (Simon, Houghton, & Aquino, 2000). Risk assessment appears to accurately predict behavior across situations, and it appears likely that if employees perceive the risk as high, they will refrain from participating in cyber misbehavior.

**Locus of Control and Risk Perception**

Individuals with internal LOC have been shown to be better able to attend to pertinent cues and disregard irrelevant signals (Gregory & Nelson, 1978). People high in external LOC are more easily swayed by false cues than internal LOC people (You, Ji, & Han, 2013). Pilots in the United Kingdom with higher internal LOC were shown to perceive more risk (Vallee, 2006). In another study of airline pilots, internal LOC led to increased safety operation behaviors,
mediated by perception of risk (You, Ji, & Han, 2013). In a study involving proofreading, internal LOC individuals were better at identifying errors in the text than people with external LOC, as their perception of subtle, random clues was superior (Wolk & DeCette, 1974). It follows that individuals high in internal LOC will experience increased risk perception, which will lead to fewer cyber misbehaviors.

**Hypothesis 2: Risk perception will mediate the relationship between locus of control and cyber misbehavior.**

![Figure 2. Model 2: Risk Perception as a Mediator](image)

While there is theoretical support that the perception of risk acts as a mediator between locus of control and cyber misbehavior, it is also plausible that risk perception could merely have a moderating effect on the relationship between locus of control and cyber misbehavior rather than being a direct link between the two. In a study of airplane safety procedures, pilots who rated risk as high demonstrated more safety operation behaviors than those who assessed risk as low (Ji et al., 2011). In a study of HIV status testing, risk perception, and framing of the test promotion as either a loss or a gain, researchers found that risk perception moderated the relationship between the framing of the promotion and the rate at which individuals chose to be tested (Hull, 2012). In another study, risk perception moderated the relationship between intention to use sunscreen and actual use of sunscreen (Craciun, Schuz, Lippke, & Schwarzer, 2010). While individuals high in internal locus of control will likely engage in fewer cyber
misbehaviors, it is possible that the amount of risk they perceive as being associated with the action will influence how their locus of control effects their behavior. Therefore, I propose the following hypothesis.

*Hypothesis 3: Risk perception will moderate the relationship between locus of control and cyber misbehavior.*

![Figure 3. Model 3: Risk Perception as a Moderator](image)

It is also possible that a direct relationship exists between locus of control and cyber misbehavior, but that there is no effect of risk perception on cyber misbehaviors. Almost any human endeavor involves some risk; just because people perceive an element of risk involved in an activity does not mean that they will not engage in that behavior (Panno, Lauriola, & Pierro, 2015). It is possible that people will engage in dangerous cyber behavior even while aware of the risks. While higher internal locus of control may lead to a perception of greater risk, it could be that this is not what drives the decrease in cyber misbehavior but rather the idea that the individual is responsible for the repercussions of their own behaviors. An additional model should examine the relationship between locus of control and risk perception while at the same time accounting for a link between locus of control and cyber misbehavior.

*Hypothesis 4: Higher internal locus of control will be associated with greater perception of risk and a lower level of cyber misbehaviors.*
As indicated previously, theory supports the idea that individuals higher in internal locus of control will exhibit fewer cyber misbehaviors, most likely through both a direct effect of locus of control on cyber misbehavior and through a relationship mediated by the perception of risk. Individuals high in internal locus of control have been shown to perceive more risk than those higher in external of locus of control (Vallee, 2006), and the perception of risk has been shown to lead to safer behaviors (You, Ji, & Han, 2013). Therefore, I propose the following hypothesis.

**Hypothesis 5**: Higher internal locus of control will be associated with greater perception of risk and a lower level of cyber misbehaviors. Greater perception of risk will also be associated with lower levels of cyber misbehaviors.
Risk Perception and Sensation Seeking

Simply existing in the world requires a certain amount of risk. Our earliest risk-taking ancestors hunted and felled the mastodon and survived to procreate, while the more risk-averse stayed safely in their caves and starved. Maybe we are somewhat hardwired for risk. But sharing a password with a coworker is not going to ensure continued survival, and the information gained by opening an email from an insecure source is probably not vital to one’s well-being. Of course, in order to make an assessment of the risk involved before deciding on a course of action, the individual must perceive the situation as containing an element of risk. Evidence suggests that people who are high in the sensation seeking personality trait may be less sensitive to risk (Roberti, 2004). Sensation seeking is a trait that is defined as a need for novel experiences and physiological arousal, along with the willingness to engage in risk to obtain such experiences and arousal (Zuckerman, 2007). Chen, Wang, Harris, and Rao (2011) found a correlation of $r = -0.12$ between sensation seeking and email risk perception, with email risk perception operationalized by three items questioning how risky and potentially loss evoking the participant believes opening emails to be. Another study found a correlation of $r = -0.60$ between sensation seeking and danger assessment, as well as a correlation of $r = 0.70$ between sensation seeking and attitude toward risk, with a higher score on attitude toward risk indicating a greater likelihood of engaging in risky behavior (Franken, Gibson, & Rowland, 1992). However, Horvath and Zuckerman (1993) found risk appraisal to be a consequence of risky behavior rather than a mediator between sensation seeking and risky behaviors. Risk appraisal for novel activities has been shown to be negatively related to sensation seeking, in that high sensation seekers assess the risk of behaviors with which they have no experience as lower than do individuals low in sensation seeking (Zuckerman, 1979). However, according to Horvath & Zuckerman (1993), it
appears that high sensation seekers experience a reduction in their perception of risk with increased familiarity with the experience, while low sensation seekers remain uncertain and apprehensive. Horvath and Zuckerman (1993) suggest that it is also possible that high sensation seekers pay less selective attention to the negative consequences of the behaviors and attend more to the rewards of the activity. Finding risk perception to be a consequence of risky behavior rather than a mediator between sensation seeking and risky behavior was unexpected by Horvath and Zuckerman (1993), and it is interesting to test these models regarding cyber behaviors. Therefore, I test two competing models, one with cyber risk perception mediating the relationship between sensation seeking and cyber misbehavior, and one with cyber misbehavior mediating the relationship between sensation seeking and cyber risk perception. My research questions are as follows.

*Research Question 1: Does cyber risk perception mediate the relationship between sensation seeking and cyber misbehavior?*

![Figure 6. Exploratory Model A: Cyber Risk Perception as Mediator](image)

*Research Question 2: Does cyber misbehavior mediate the relationship between sensation seeking and cyber risk perception?*
Figure 7. Exploratory Model B: Cyber Misbehavior as Mediator
CHAPTER TWO:

METHOD

Participants

Participants were recruited through Amazon Mechanical Turk. Studies have shown Mechanical Turk data to have good test-retest reliability (Holden, Dennie, & Hicks, 2013) as well as scale reliability (Buhrmester, Kwang, & Gosling, 2011). These research participants perform well in attention and concentration checks (Berinsky, Huber, & Lenz, 2010) and have been shown to replicate findings from previous studies (Horton, Rand, & Zeckhauser, 2011). Screening criteria were as follows: participants were required to work a minimum of 20 hours weekly with at least 3 of those hours involving working on a computer.

Procedure

The study was posted on Amazon Mechanical Turk’s website and individuals who chose to participate received a link to an external Qualtrics survey. Potential participants were first presented with a consent form, which they were asked to read and acknowledge. After giving consent, participants answered a series of demographic questions such as age, sex, and education attained, as well as the number of hours worked weekly and the number of hours worked weekly on a computer. This was followed by the measures for locus of control, risk perception, cyber misbehavior, and sensation seeking. Finally, several brief questions regarding the participants’ experiences with cyber malfeasance were posed. Items were presented in this order to prevent the possibility of order effects due to priming. Participants who have experienced cyber malfeasance might be primed to respond more cautiously to the questions regarding perception
of risk. Likewise, if participants reported their cyber misdeeds prior to responding to questions regarding their perception of risk, this may affect the amount of risk they perceive. It seemed prudent to ask the more subjective and easily influenced questions before the more concrete questions regarding behavior and experience. Any possibility of order effects due to lack of counter balancing seems outweighed by these concerns. After completion of the survey, participants were provided with a unique code they could enter to receive compensation of $.75. Participants were assured that the information obtained was confidential and for research purposes only, and that no names or identifiable information was connected to their responses.

**Measures**

**Locus of Control.** Locus of control was measured using Rotter’s (1966) Locus of Control Scale. This measure consists of 29 forced-choice pairs for which the respondent must choose one of two statements, one of which is internally oriented and the other of which is externally oriented. An example of an item is “Many of the unhappy things in people’s lives are partly due to bad luck” (external) versus “People’s misfortunes result from the mistakes they make” (internal). See Appendix A for the full list of items.

**Risk Perception.** While risk perception scales exist in such areas as substance abuse and aviation, among others, no such measure exists for cybersecurity risk perception. Therefore, the six general risk perception items were pulled from Hunter’s (2003) aviation risk perception scale, and six additional items relating to cybersecurity were created. This rating scale is measured on a Likert scale with 1 = “Extremely unlikely” and 7 = “Extremely likely” with a lower score indicating a higher level of risk perception. An example of a general risk perception item is “Climb up a 10-foot ladder to replace an outside light bulb.” An example of a cyber risk perception item is “Insert a USB drive that you found in the parking lot into your computer.” A
higher score indicates a lower perception of risk. See Appendix B for the general risk perception items and Appendix C for the cyber risk perception items.

**Cyber Misbehavior.** The six security risk behavior items from Stanton (2005) et al.’s taxonomy of end-user security behaviors were utilized as a measure of cyber misbehavior. One such item is “I have shared my work account user name or password with a friend or coworker.” A higher score indicates a higher level of cyber misbehavior. See Appendix D.

**Sensation Seeking.** Sensation seeking was measured using ten items representing sensation seeking/risk taking/thrill seeking from the International Personality Item Pool (Goldberg, 1992). An example of an item is “Am willing to try anything once.” Participants were asked to indicate on a Likert scale where 1 = “Very Inaccurate” to 5 = “Very Accurate” how much the statement applies to them. A higher score indicates a higher level of the sensation seeking trait. For the full list of items, see Appendix E.

**Experience with Cyber Malfeasance.** An individual’s experience shapes their subjective expectancies, and as LOC is predicated on expectancy theory, it would follow that one’s sense of control would stem from personal experience. In a study of computer users, those who had experienced cyber safety hazards exercised greater security intentions (Tsai et al., 2016). Prior experience with virus infections significantly predicted college students’ intentions to use virus protection (Lee, LaRose, & Rifon, 2008). In a study of Turkish students, academics, and administrators who used information systems, education level and information security awareness training were related to safer user behavior (Ögütçü, Testik, & Chouseinoglou, 2016). Therefore participants were asked how many years they had regularly used a computer at work, as well as whether they or anyone close to them had ever been the target of a phishing scam, had
their information technology compromised, or been the victim of any other type of cyber crime. These questions are detailed in Appendix F.

**Demographics.** Finally, participants were asked to report their age, sex, level of education, and job tenure. See Appendix G.

**Data Analysis**

Before beginning the analysis, the data needed to be examined for abhorrent response patterns. Out of 250 participants, 14 failed the attention check, two neglected to answer the question asking for their consent, and two admitted to hurrying through the survey. In a pilot study, I had previously determined the survey could not be properly completed in less than 4 minutes and 30 seconds, so responses under this limit were deleted from the data. There were 23 such cases. The final question of the survey asked participants if they had experienced any problems with the survey. This was intended to ensure that all the procedures and questions were clear and that no issues arose that might affect the quality of the data. Most participants either left this question blank or answered to the effect that there had been no problems and the survey was fine. A few people said “thank you,” a couple participants said it had been fun, and one participant said I should pay more. Only one person reported technical difficulties that had not allowed him to complete a page of the survey. His data was deleted. Another participant who inexplicably left a large amount of the survey blank was also dropped. The final sample was 207. According to MacCallum, Browne, and Sugawara’s (1996) estimation of minimum sample size in structural equation modeling, approximately 178 participants are required to achieve a power of 0.80, so this is an adequate sample size. There were 78 response items required from each participant, and 11 participants left at least one item blank.
Next, a factor analysis of each of the constructs was executed in SPSS using principal components as the extraction method and direct oblimin rotation. With one exception that will be discussed momentarily, only one factor was extracted for each set of items, meaning the items measuring each construct loaded onto that construct only (Browne, 2001). The reliability of all the scales was assessed, as well as the effect of the deletion of each item on the reliability of the scale. The reliabilities of the scales were over Nunnaly’s (1978) recommended 0.70 with the reliability of locus of control at $\alpha = 0.75$, cyber misbehavior at $\alpha = 0.79$, and sensation seeking at $\alpha = 0.74$. With the deletion of each item, the reliability of each scale decreased, indicating the efficacy of all items. The factor analysis indicated that all the measures utilized in the study were good, with the exception of the risk perception scale. The 12 risk perception items appeared to be measuring three distinct constructs, with the first two general risk perception items loading on one factor, the last four general risk perception items loading on another, and the six cyber risk perception items loading on a third factor. The reliability of the six cyber risk perception items was $\alpha = .76$, with the deletion of any one item decreasing the reliability. As the general risk perception items appear to be measuring other constructs and also had a reliability below Nunnaly’s (1978) recommendation of 0.70, I decided to reduce my measure of risk perception to the six cyber risk perception items. Henceforth this construct and scale will be referred to as cyber risk perception. To address the reason the six general risk perception items worked along with aviation risk perception items to make up Hunter’s (2003) aviation risk perception scale, but do not work effectively in conjunction with cyber risk perception items, one possibility comes to mind. All of Hunter’s (2003) items—both general and aviation specific—concern corporeal risk, while the cyber risk perception items refer to risk of cyber harm or compromised data. It is likely that a threat to one’s physical being is perceived differently than a potential breach of
information systems. Additionally, most of the cyber risk involved would affect the participants’ employer, rather than the participants themselves. It is not surprising that the perception of physical risk is a different construct than the perception of risk to an employer’s data.

After the data was clean and the reliability of the measures was established, it was time to analyze the data. In this study, structural equation modeling using Mplus (Muthen & Muthen, 1998-2012) was utilized to estimate parameters and assess the fit of the models. Structural equation modeling is a method used to analyze and assess the underlying structural relationship between manifest or measured variables and latent or unmeasured variables (Bollen, 1989). Structural equation modeling includes path analysis, confirmatory factor analysis, partial least squares path modeling, and latent growth modeling. It is generally linear and cross-sectional in nature, with the exception of growth curve modeling. Structural equation modeling makes it possible to test competing theoretical models that each represent a different pattern of the possible relationship among the variables, and the researcher can then compare the fit of these models in order to select that which best represents the data (MacCallum, Browne, & Cai, 2006). A single tested model with reasonable fit indices can at best be said to be a plausible interpretation of the data; meaningful theory testing requires going beyond null hypothesis testing and instead examining at least two comparative theories (Clarke, 2011).

Bauer (2017) states that a primary advantage of structural equation modeling is that the researcher can obtain an unbiased estimate of the effects between the predictors and the outcomes due to the absence of measurement error in the latent variables. In this study, cyber misbehavior is investigated as a function of locus of control and risk perception. By using structural equation modeling, with multiple indicator measures for each variable assessing the latent construct of the variable, I was able to get unbiased estimates of the effects of locus of
control, sensation seeking, and risk perception on cyber misbehavior. This assumes the structure that has been specified in the model is accurate, which leads to a second advantage of structural equation modeling (Bauer, 2017).

With structural equation modeling we are able to evaluate the structure of our models by comparing their fit to the patterns observed in our data (Bauer, 2017). When we test whether our model is consistent with the data, we determine if the model we have specified is likely to be plausible in the population. You are testing to see whether relationships between the indicator variables really are accounted for by the associations between the latent variables. Using theory and previously tested information from the literature, I constructed models that made the most theoretical sense. Using structural equation modeling, I was able to compare these models to the associations that exist in my data, to see how plausible my hypothesized models are (Bauer, 2017). There is no such thing as a “true” or “correct” model; there will always be other factors involved that you are not accounting for. I imagine that a “true” model of even the simplest relationship would be incredibly complex. But even though we cannot model the truth, we can establish practical and useful models. If we find a model has good fit, this provides valuable information about the relationships that most likely exist in the population, regardless of whether this gives us a complete picture or even an entirely correct picture. Beyond establishing plausibility, we can compare the fit of various competing plausible models to determine which model best fits the patterns in the data. When used in this manner, structural equation modeling is a valuable tool. While all my models have theoretical support, some were found to be more practical than others. This information is of value as it leads to further knowledge of the relationships that exist between cyber misbehaviors and other constructs. Especially in a field as nascent as cybersecurity, structural equation modeling is a good statistical tool to use in
investigating possible patterns of behavior. With so much still to discover in the field of cybersecurity, there is a smaller body of theoretical knowledge to draw upon than there may be in other areas, but as we learn more, we will be able to hypothesize and test more complex models.

A third advantage of structural equation modeling is the fact that we are able to use it to specify complex theoretical structures (Bauer, 2017). In the behavioral sciences, hypotheses can be quite complicated, and other statistical analysis techniques are not able to test them in the way that structural equation modeling can. For example, Bauer (2017) states that structural equation modeling can establish a “causal chain,” where one factor may have an effect on another variable through a third variable, which is basically mediation. These effects are difficult to test using regression and other techniques. While this study does not contain very complicated models, structural equation modeling is able to generate parameter estimates and provide measures of statistical and practical fit.

Structural equation modeling can also have its drawbacks. I believe most of these are due to misuse of the technique rather than problems with the technique itself. Conceptualization of a model should always originate from theory, and if the data are found to fit the model poorly, the buck stops there. There should be little modification of the model in an attempt to find better fit. While nonsignificant results in experimentation and poorly fitting models in structural equation modeling are disappointing, there is something to be learned from them as well. At least you know what didn’t work! Even if you have good fit, you can make the mistake of then assuming you have found the “correct” model. At best all you can claim is a model which is plausible. Good models can be very useful, but there is always a limit to what they can tell us. As long as structural equation modeling is properly executed and the results are properly interpreted, I
believe the advantages of structural equation modeling far outweigh the drawbacks. Most problems seem to be in the domain of the researcher rather than the fault of the technique. No method of statistical analysis is perfect; it is important to choose the one that best suits the situation and to implement it correctly.

In the first part of the study I had five competing models that I compared to determine which best fit the data. The first step was to run the analysis of each hypothesized model. The fit of each model was assessed based on the goodness-of-fit statistics $\chi^2$, Comparative Fit Index (CFI), Tucker Lewis Index (TLI), Standardized Root Mean Square Residual (SRMR), Root Mean Square Error of Approximation (RMSEA), and Confidence Intervals.

A significant $\chi^2$ is an indication that the model does not hold in the population, but this statistic has severe drawbacks. Byrne (2012) states that large samples are important for precise parameter estimates, however, the $\chi^2$ tends to be larger when the sample size is large and the model does not hold (Jöreskog & Sörbom, 1993), so it is acceptable to have a significant $\chi^2$ and still assume goodness of fit if the other fit statistics show a good representation of the data.

Other fit statistics to examine include the Comparative Fit Index (CFI) and the Tucker-Lewis Index (TLI), both of which should be at or above .95 as the generally acceptable point, or above .90 as a slightly more relaxed criterion (Browne & Cudeck, 1993). These are incremental indices of fit, and when comparing the fit of the various models the CFI and TLI should increase as the fit of the model improves.

The Standardized Root Mean Square Residual (SRMR) represents the average of all the standardized residuals, and will be from 0 to 1, and in a model with good fit will usually be below 0.05. The SRMR indicates the value of the average error at which the model explains the correlation. The Root Mean Square Error of Approximation (RMSEA) indicates the discrepancy,
per degree of freedom, between how well the model would fit the population covariance matrix if it were possible to access it (Byrne, 2012). The RMSEA should optimally be less than .05, but Byrne states that Brown and Cudeck (1993) maintain that values as high as .08 are reasonable, and MacCallum et al. (1996) asserts that values ranging from .08 to .10 indicate mediocre fit, with those greater than .1 indicating poor fit. Moreover, we can build confidence intervals around the RMSEA. The 90% confidence interval can be interpreted to mean that we can be 90% confident that the true RMSEA value in the population will fall between the values obtained, so you can state with 90% assurance that the true value of the RMSEA for the population is no larger than the high end of the confidence interval. An RMSEA value can be acceptable yet have an unacceptably wide range in the confidence interval. SRMR and RMSEA are absolute indices of fit and should decrease as the comparative fit of the model improves.

After assessing the fit of each model to determine if the model is a plausible representation of the data, the fit of the nested models is compared. Additionally, the significance of the parameter estimates is determined and the direction and value of the beta weights assessed.
CHAPTER THREE:

RESULTS

Demographics

The sample of 207 individuals was 68.2% male, 31.4% female, and fewer than 1% preferred not to state their sex. The average age of the participants was 36.2 years ($SD = 11.1$). Fewer than 1% of participants had some high school education, 4.3% had a high school diploma or GED, 14.5% had some college education, 1.2% had trade/technical/vocational training, 7.8% has an associate’s degree, 49% had a bachelor’s degree, 16.5% had a master’s degree, 4.3% had a professional degree, 1.6% had a doctoral degree, and fewer than 1% preferred not to answer the question regarding their education. The average number of hours worked per week was 39.7 ($SD = 9.8$), the average number of hours spent weekly on a computer was 28.6 ($SD = 12.36$), and the mean number of years the participants had been working on a computer was 9.3 ($SD = 7.2$). Twenty-seven percent stated that they or someone they knew had previously been a victim of a phishing scam, while 21.3% answered maybe to that question and 51.6% stated that they had not. Twenty-eight percent said yes, 16.3% said maybe, and 55.5 % said no when asked if they or someone close to them had ever had their information technology compromised. Twenty-eight percent answered yes, 12.7 % answered maybe, and 59.2 % said no when asked if they or anyone close to them had ever been the victim of any other type of cyber crime.

Fit of Hypothesized Models

According to the first hypothesis, high internal locus of control would lead to a decrease in cyber misbehavior. In this model, the chi-square was nonsignificant—which is good—at $\chi^2$
(14, N = 207) = 14.98, p = 0.38. Additionally, CFI = 0.996 and TLI = 0.995, both of which indicate a good representation of the data. In this model, the SRMR = 0.033 and the RMSEA = 0.018, which are both excellent. The confidence interval for this model is [0.00, 0.071], so we can be 90% sure that the true value in the population is within that range. This means that we can say with 90% assurance that our true value is no higher than 0.071 for the RMSEA. Overall, the fit of Model 1 is very good and this model is a plausible representation of the data. The parameter estimate for this relationship is significant, with a beta weight of -0.866. This indicates that increased internal locus of control leads to decreased engagement in cyber misbehaviors, and decreased internal locus of control leads to increased engagement in cyber misbehaviors, so Hypothesis 1 is supported. See Table 1 for fit indices. See Figure 8 for standardized estimates.

Figure 8. Standardized Estimates for Model 1: Relationship between higher internal locus of control and cyber misbehavior.
According to Hypothesis 2, cyber risk perception would fully mediate the relationship between locus of control and cyber misbehavior. In this model chi-square was significant at $\chi^2 (64, N = 207) = 97.94, p = 0.00$, but that could be overlooked should the other statistics prove promising. CFI and TLI are 0.949 and 0.938 respectively, and SRMR and RMSEA are 0.047 and 0.051, with a confidence interval of $[0.029, 0.070]$, which are reasonable. This model also represents a plausible fit to the data. The parameter estimates for both paths are significant, with the beta weight for the relationship between locus of control and cyber risk perception at -0.279 and for that between cyber risk perception and cyber misbehavior at 0.777. As cyber risk perception is measured on a Likert scale with low scores indicating an unlikeliness of engaging in risky behaviors, high scores on the cyber risk perception scale actually represent a lower level of cyber risk perception. This means that the negative relationship between locus of control and cyber risk perception indicates that as internal locus of control increases, an individual is less likely to perceive a situation as low-risk. Consequently, a person who perceives a situation as low-risk is more likely to engage in cyber misbehaviors. Thus, cyber risk perception mediates the relationship between locus of control and cyber misbehavior and Hypothesis 2 is supported. See Table 1 for fit indices. See Figure 9 for standardized estimates.
In Hypothesis 3, it was posited that cyber risk perception would moderate the relationship between locus of control and cyber misbehavior. The fit statistics for this model are $\chi^2 (24, N = 207) = 23.53, p = 0.49$, CFI = 1.00, TLI = 1.00, SRMR = 0.030, and RMSEA = 0.00 [0.000, 0.055], which is excellent. The parameter estimate for this moderation path is significant and the weight is -0.325. This means that with the increase of the perception of a situation as being low-risk, the influence of internal locus of control in lowering engagement in cyber misbehaviors decreases. Hypothesis 3 is supported. See Table 1 for fit indices. See Figure 10 for standardized estimates.
Hypothesis 4 states that internal locus of control will be associated with greater perception of cyber risk as well as a lower level of cyber misbehavior. Chi-square is significant at $\chi^2(64, N = 207) = 189.32, p = 0.00$, CFI and TLI are 0.813 and 0.772, SRMR is 0.173 and RMSEA is 0.097, with a confidence interval of [0.081, 0.113]. This is very poor and Model 4 is not considered further. The fit of this model is likely so poor because, as previously indicated in Model 2 and as we will see momentarily in Model 5, quite a strong relationship is indicated between cyber risk perception and cyber misbehavior. Therefore, the absence of a path between these two constructs most likely accounts for the poor fit of the model. See Table 1 for fit indices. See Figure 11 for standardized estimates.
Figure 11. Standardized Estimates for Model 4: Internal locus of control leading to decreased cyber misbehavior; internal locus of control leading to lower perception of low cyber risk.

Finally, Hypothesis 5 asserted that higher internal locus of control would be associated with both greater perception of cyber risk and lower levels of cyber misbehavior, as well as perception of cyber risk being associated with lower levels of cyber misbehavior. This is the partially mediated model. The fit is quite good with $\chi^2 (63, N = 207) = 97.24$, $p = 0.00$, CFI = 0.949, TLI = 0.937, SRMR = 0.047, and RMSEA = 0.051 [0.030, 0.071]. The parameter estimates between locus of control and cyber risk perception and cyber risk perception and cyber misbehavior are significant and the weights are -0.280 and 0.780 respectively. However, there is a nonsignificant parameter estimate for the relationship between locus of control and cyber misbehavior in this model, with a beta weight of 0.007. What this indicates is that while higher cyber risk perception mediates the relationship between higher internal locus of control and less engagement in cyber misbehavior, with the introduction of cyber risk behavior to the model,
locus of control no longer has a significant direct effect on cyber misbehavior. When locus of control and cyber misbehavior are the only constructs in the model (Model 1), there is a significant relationship between the two, but when cyber risk perception is brought into the model, locus of control no longer explains a significant amount of the variance in cyber misbehavior. Therefore, Model 5 is partially supported. See Table 1 for fit indices. See Figure 12 for standardized estimates.

Figure 12. Standardized Estimates for Model 5: Internal locus of control leading to decreased low cyber risk perception; low cyber risk perception leading to increased cyber misbehaviors; nonsignificant path between locus of control and cyber misbehavior.

Fit of Exploratory Models

The second part of this study involved two research questions concerning sensation seeking. Very little is known regarding the relationship between sensation seeking, cyber risk perception, and cyber misbehaviors, so no hypotheses were posed. The purpose was to determine whether cyber risk perception was more likely to mediate the relationship between sensation seeking...
seeking and cyber misbehavior, or if cyber misbehavior was more likely to mediate the relationship between sensation seeking and cyber risk perception. These relationships were modeled including an additional direct path between sensation seeking and cyber misbehavior in the first research question, and between sensation seeking and cyber risk perception in the second research question. Upon investigating these relationships in the course of this study the decision was made to propose and test two additional models, by deleting the path between sensation seeking and cyber misbehavior in the first model and between sensation seeking and cyber risk perception in the second model, resulting in two sets of nested models.

As these models are nested within one another, the first model—Exploratory Model A—will be the model with cyber risk perception mediating the relationship between sensation seeking and cyber misbehavior, as this is the simplest representation of the relationship between these variables. The fit of this model was not good, with $\chi^2 (207, N = 207) = 439.91, p = 0.00$, CFI = 0.833, TLI = 0.813, SRMR = 0.073, and RMSEA = 0.074 [0.064, 0.083]. The parameter estimates are significant, with the weight for the path between sensation seeking and cyber risk perception at 0.629 and that for the path between cyber risk perception and cyber misbehavior at 0.784. See Table 2 for fit indices. See Figure 13 for standardized estimates.
Figure 13. Standardized Estimates for Exploratory Model A: Higher sensation seeking trait leading to increased perception of low cyber risk; lower cyber risk perception leading to increased cyber misbehavior.

Exploratory Model B adds a direct path from sensation seeking to cyber misbehavior. The fit of this model is $\chi^2(206, N = 207) = 470.96, p = 0.00, \text{CFI} = 0.833, \text{TLI} = 0.813, \text{SRMR} = 0.073, \text{and RMSEA} = 0.079 \,[0.069, 0.088]$, which is pretty poor. The parameter estimates for the paths between cyber risk perception and cyber misbehavior and between cyber risk and sensation seeking are significant, and the weights are 0.722 and 0.617 respectively. The additional path between sensation seeking and cyber misbehavior is nonsignificant. See Table 2 for fit indices. See Figure 14 for standardized estimates.
Figure 14. Standardized Estimates for Exploratory Model B: Higher sensation seeking trait leading to increased perception of low cyber risk; lower cyber risk perception leading to increased cyber misbehavior; nonsignificant path between sensation seeking and cyber misbehavior.

Exploratory Model C models cyber misbehavior as a mediator between sensation seeking and cyber risk perception. The fit of Model C is poor, with $\chi^2(207, N = 207) = 452.05$, $p = 0.00$, CFI = 0.823, TLI = 0.803, SRMR = 0.076, and RMSEA = 0.076 [0.066, 0.085]. See Table 2 for fit indices. The parameter estimates are significant with the weight of the path between sensation seeking and cyber misbehavior at 0.579 and the weight of the path between cyber misbehavior and cyber risk perception at 0.805. See Table 2 for fit indices. See Figure 8 for standardized estimates.
Figure 15. Standardized Estimates for Exploratory Model C: Higher sensation seeking trait leading to increased cyber misbehavior; cyber misbehavior leading to greater perception of low cyber risk.

Exploratory Model D contains a path between sensation seeking and cyber risk perception in addition to those between sensation seeking and cyber misbehavior and cyber misbehavior and cyber risk perception. The fit of Model D is not good, with $\chi^2(206, N = 207) = 478.17, p = 0.00$, CFI = 0.817, TLI = 0.795, SRMR = 0.074, and RMSEA = 0.081 [0.072, 0.091]. All paths are significant, with the weight of sensation seeking and cyber misbehavior at 0.532, sensation seeking and cyber risk perception at 0.286, and cyber misbehavior and cyber risk perception at 0.623.
Comparison of Nested Models

After assessing the fit of the models and concluding that all but Model 4 and probably the exploratory models are plausible representations of the data, I looked at the difference in chi-square between the nested models. For the five models in the first part of the study, Model 2 and Model 4 are nested within Model 5. For the chi-square difference test, the chi-square and degrees of freedom of the larger model with more parameters and fewer degrees of freedom are subtracted from those of the smaller model with fewer parameters and more degrees of freedom (Bollen, 1989). For Model 5 and Model 2, there is a nonsignificant change in chi-square of $\Delta \chi^2 = 0.71$, $p = 0.01$. The chi-square difference test indicates that there is no significant difference in the fit between Model 2 and Model 5; there is no improvement in fit when deleting the additional parameter between locus of control and cyber risk perception. However, for Model 5 and Model 4, the difference is significant at $\Delta \chi^2 = 90.67$, $p = 0.01$. The chi-square difference test
reveals a significant difference in the fit between Model 4 and Model 5, meaning that removing the parameter between cyber risk perception and cyber misbehavior decreases the fit of the model. Hence, Model 5 is superior to Model 4.

Out of all five models, Model 2 and Model 3 fit the data the best overall; it could presumably be argued either way that one eclipses the other. Model 3 has somewhat better fit indices, but a moderation model cannot really be compared to a model of mediation, and Model 2 has other comparative models against which it stands out as superior. Model 1 actually has slightly better fit than Model 2; however, the fact that cyber risk perception is shown in subsequent models to have such a strong relationship with cyber misbehavior indicates that this model can’t practically be said to be the better model. Model 5 further illustrates this fact, as when cyber risk perception is brought in as a mediator between locus of control and cyber misbehavior the direct path between locus of control and cyber misbehavior becomes insignificant. While Model 3 has better fit than Model 2, I would argue that in light of the information that can be obtained from the remaining three models in support of Model 2, Model 2 can be said to be the superior model.

For the exploratory models, Model A is nested within Model B, and Model C is nested within Model D. For Model B and Model A, the difference in chi-square is significant at $\Delta \chi^2 = -31.05$ (1), $p = 0.01$, therefore removing the parameter between sensation seeking and cyber misbehavior significantly improves the fit, and Model A is superior to Model B. The change in chi-square is also significant in the difference between Model D and Model C at $\Delta \chi^2 = -26.12$ (1), $p = 0.01$. This indicates that the deletion of the parameter between sensation seeking and cyber risk perception improves the fit of the model and Model C is preferable to Model D.
As the exploratory models exhibited mediocre fit at best, it would be unwise to draw conclusions based on these models. However, if anything were to be determined it would be that it may be slightly more likely that the sensation seeking trait leads to a state of lower perception of risk, which in turn leads to fewer cyber misbehaviors, rather than the sensation seeking trait leading to the engagement in more cyber misbehavior, which would then lead to a lowered state of the perception of risk. It is interesting to note, however—as cautiously as we must do so considering the fit of the models—that the difference in fit for these models is not huge. Therefore, there may be some credence to the idea that engagement in cyber misbehaviors could sometimes—or for some individuals--be the antecedent to a lower perception of risk, rather than vice versa.
CHAPTER FOUR:

DISCUSSION

Based on theoretical evidence that internal locus of control is generally associated with higher interpretation of risk and more cautious behavior—as has been found in areas such as aviation, health, and construction—this study sought to investigate whether these findings would translate into the realm of cybersecurity and cyber-related perceptions and behaviors. Several models were posited, predicated on the idea that internal locus of control would lead to greater perception of cyber risk, and that greater perception of cyber risk would lead to fewer cyber misbehaviors, relationships favored with support from theory.

The moderation model (Model 3) had excellent fit, indicating that perception of cyber risk increases the effect that internal locus of control has on lessening cyber misbehaviors. Additionally, it was found in Model 2 and Model 5 that internal locus of control increases the perception of cyber risk, and increased cyber risk perception is strongly related to lesser engagement in cyber misbehavior. There appears to exist a relationship between an individual’s feeling that they are in control of their environment and the amount of risk that individual will intuit as existing in that environment, which lowers the extent to which the individual will participate in dangerous behavior. This has been indicated in such domains as sunscreen use, athletic endeavors, and construction work, and now it seems it can be said for cybersecurity behavior as well. If an employee believes that they have mastery over the work environment and that they can control the work-related rewards and punishments that come to them, they will be more likely to intuit cyber danger, and less likely to engage in potentially hazardous activities.
that threaten the cybersecurity of the organization—behaviors that could harm the organization and threaten the rewards the individual expects to receive from the organization as a result of their labors. The person who is higher in external locus of control sees themselves as non-influential and does not believe they can control what happens to them and what rewards and punishments they will receive. This person will not discern the risk involved and will be more likely to engage in dangerous behavior. They may not feel the need to be careful in order to protect themselves and their organization, because they don’t feel that their actions have much impact on the world around them and on the rewards and punishments they receive. While it is probably not practical to utilize locus of control as a selection variable, it might be possible that people high in internal locus of control could be placed in the positions for which safe cyber hygiene is most imperative, or at least to keep individuals very high in external locus of control out of these positions. Since training in cyber awareness and proper cyber hygiene is a primary method of promoting cyber safety, it is possible that people high in internal locus of control would be better suited for designing and implementing these training courses than people lower in internal locus of control; it may be that they will be better able to impart the importance and individual responsibility of cyber hygiene than someone who does not feel as much of a sense of personal responsibility. Since it appears that individuals who have a feeling of personal agency in their environment and personal accountability for their own situations—who see themselves as masters of their own fate—are more likely to perceive risk and engage in less cyber misbehavior, organizations should promote the idea of personal responsibility in cyber safety.

Model 1 indicated that internal locus of control has a modest association with decreased cyber misbehaviors, yet when cyber risk perception was added as a mediator between locus of control and cyber misbehavior in Model 5, the path between locus of control and cyber
misbehaviors became nonsignificant and the path between cyber risk perception and cyber misbehaviors was quite strong. What this implies is that while the trait locus of control may have some direct effect on the cyber behavior of an individual, the state of risk perception is a very important mediator in this relationship.

This is interesting and important because an organization may be able to change employees’ attitudes and states, such as their perceptions, while traits such as locus of control are more static and immutable. In this instance, the relationship between the trait (locus of control) and the behavior (cyber misbehavior) is mediated by a state (cyber risk perception). This is encouraging because as mentioned previously in this paper, attitudes lead to behaviors, and good cyber training programs, cybersecurity-oriented leadership, and a strong culture of cyber safety could lead to an attitude of cyber compliance in employees, which could then facilitate good cyber hygiene. This paper previously addressed the assessment of risk, and the fact that people will often gauge the level of risk at least partially based on the perceived payoff for engaging in that risky behavior. If organizations can lower the standards by which situations will be perceived as risky, and raise the standards for what would be perceived as an adequate reward for engaging in risk, they have every hope of changing their employees’ attitudes toward risky behavior and their level of engagement in these behaviors.

While the fit for the sensation seeking models could generously be said to be merely mediocre, the comparative fit of the models still tells an interesting story. The fit of the models utilizing cyber risk perception as a mediator between sensation seeking and cyber misbehavior was only very slightly better than that of the models with cyber misbehavior as a mediator between locus of control and cyber risk behavior. This implies that it may be almost as likely that the level of risk employees discern depends on how much they engage in cyber misbehaviors as
it is likely that the degree of cyber misbehavior employees engage in depends upon how risky they think these behaviors are. As discussed earlier in this study, the reasons why an employee might or might not engage in risky behavior are complicated and varied. It could be, however, that employees partaking in risky behaviors that result in no repercussions could have dangerous consequences for organizations in that this may lower the perception of risk, perhaps even for employees who do not initially engage in these behaviors themselves but who observe others doing so without negative consequences. Watching a co-worker load sensitive information onto a USB drive so they can take their day’s work to the beach, and then seeing them return the next day with a tan and a smile and no repercussions, could lower the perception of risk for both the beach-going employee and co-workers. Organizations should not only prohibit such dangerous activity but should actively monitor and enforce the rules and punish those who engage in unsafe cyber actions, regardless of whether or not the activity had negative consequences. If the potential punishment for sloppy cyber behavior is greater than the possible reward, employees will likely perceive the risk as higher and be less likely to participate in poor cyber hygiene.

**Implications**

Several implications of note can be inferred from this study. The first came to light early in the analysis with the validation of the measures. The fact that general risk perception items cannot be combined with cyber risk perception items to make one scale measuring the same construct—as has been done in aviation and other fields—has implications for how we measure the construct of cyber risk and how it is perceived. Cyber risk perception is in its infancy such that there is not yet a recognized scale for it, yet as cybersecurity research advances, accurately measuring an individual’s perception of cyber risk will surely be crucial, given what the literature tells us regarding the prevalence of attitudes influencing behaviors.
Indeed, this study supports the theoretical supposition that attitude influences behavior. In the study, the trait locus of control was found to be related somewhat to the behavior of decreased cyber misbehaviors, but only when no state or attitude was included in the model. When the state of cyber risk perception was brought into the model, the trait locus of control no longer had a significant relationship with the cyber behavior. This tells us that maybe cyber researchers should be looking more for what they can influence and potentially change—such as attitudes and intentions—rather than static personality characteristics and individual traits. It might be beneficial for organizations to place individuals who are high in internal locus of control in positions of leadership, as this state of risk perception might ignite within the work teams, but it is the attitudes of its employees that organizations should probably be trying to influence.

**Limitations and Future Research**

One drawback of this research is related to the fact that cybersecurity is such a nascent field and so little is yet known about the relationships between people’s cognitions, beliefs, attitudes, and actions regarding cyber behavior. This leads the hypotheses posited and the models tested in this study to be possibly overly simple in design. The relationship between locus of control, cyber risk perception, and cyber misbehavior is likely much more complicated than illustrated in these models. There are sure to be additional factors that have not been taken into consideration here.

Additionally, issues could exist within the SEM technique utilized. Although most of the models showed good fit, all we can interpret from this is that these models are plausible representations of the data. Even the best model in this study is not the “correct” model, and as discussed above there are likely other factors involved in these relationships. As it was
discovered that the moderation model (Model 2) and the mediation model (Model 3) have the superior fit out of those tested, it would be productive to investigate how a moderated mediation model would fare.

It is also appropriate to give some doubt to the self-reported nature of the data. It is possible that people would rather not remember their cyber misdeeds and unintentionally under-reported them, or perhaps they simply lied. Additionally, the fact that the study is cross-sectional makes it difficult to prove that locus of control is necessarily leading to higher risk perception, or that perception of cyber risk leads to fewer cyber misbehaviors.

In fact, that is something that could be investigated in future research. Although it would be difficult to conduct a study of this topic experimentally, models could be tested looking at cyber misbehavior as a possible antecedent to cyber risk perception. The research questions regarding sensation seeking indicate that this appeared to be almost as likely a direction as the perception leading to the behavior. It would be beneficial to either rule this out regarding locus of control, or if it was found to be plausible, to open up another important avenue of exploration regarding cybersecurity behavior. Further research could also be conducted in an expansion of the models with additional constructs of interest.

**Conclusion**

This study investigated several constructs that had not yet been explored in the arena of cybersecurity—locus of control, risk perception, and sensation seeking—and their relationships with cyber misbehavior. Results indicate that while internal locus of control has a relationship with the curtailing of cyber misbehaviors, it is the perception of cyber risk stemming from this trait that has the larger effect on lowering the rate of cyber misbehaviors. This suggests that it is the state or attitude that drives the behavior in this instance, not the trait. This is helpful to know
because it will be much easier to design training programs and other initiatives in an attempt to change employees’ attitudes toward cyber risk than it would be to try to change their inherent traits or to attempt to hire people based on these traits.
REFERENCES


Dreibelbis, R. (2016). It’s more than just changing your password: Exploring the nature and antecedents of cyber-security behaviors.


Organizational Behavior & Human Performance, 16(2), 259-279.

Meta-analytic comparisons of integrative behavioral outcomes and time sequences. 
Academy of Management Journal, 49(2), 305-325.

He, X. (2014). The role of health locus of control and self-efficacy beliefs in sunscreen use: 
Evidence from 2012 Health Information National Trends. The Journal of Cancer 

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.


Hofstede, G. (1986). The usefulness of the “organizational culture” concept. Journal of 
Management Studies, 23(3), 253-257.

120 on Amazon’s Mechanical Turk. Computers in Human Behavior, 29, 1749–1754


experiments in a real labor market. Experimental Economics, 14, 399–425.

Personality and Individual Differences, 14(1), 41-52.


Macey, W.H. & Schneider, B. (2008). Engaged in engagement: We are delighted we did it. *Industrial and Organizational Psychology: Perspectives on Science and Practice, 1*(1), 76-83.


APPENDIX A

Rotter's Locus of Control Scale Rotter (Rotter, 1966)—measures locus of control (LOC)

For each question select the statement that you agree with the most

1. a. Children get into trouble because their parents punish them too much.
b. The trouble with most children nowadays is that their parents are too easy with them.

2. a. Many of the unhappy things in people's lives are partly due to bad luck.
b. People's misfortunes result from the mistakes they make.

3. a. One of the major reasons why we have wars is because people don't take enough interest in politics.
b. There will always be wars, no matter how hard people try to prevent them.

4. a. In the long run people get the respect they deserve in this world.
b. Unfortunately, an individual's worth often passes unrecognized no matter how hard he tries.

5. a. The idea that teachers are unfair to students is nonsense.
b. Most students don't realize the extent to which their grades are influenced by accidental happenings.

6. a. Without the right breaks one cannot be an effective leader.
b. Capable people who fail to become leaders hive not taken advantage of their opportunities.

7. a. No matter how hard you try some people just don't like you.
b. People who can't get others to like them don't understand how to get along with others.

8. a. Heredity plays the major role in determining one's personality.
b. It is one's experiences in life which determine what they're like.

9. a. I have often found that what is going to happen will happen.
b. Trusting to fate has never turned out as well for me as making a decision to take a definite course of action.

10. a. In the case of the well prepared student there is rarely if ever such a thing as an unfair test.
b. Many times exam questions tend to be so unrelated to course work that studying in really useless.
11. a. Becoming a success is a matter of hard work, luck has little or nothing to do with it. b. Getting a good job depends mainly on being in the right place at the right time.

12. a. The average citizen can have an influence in government decisions.

b. This world is run by the few people in power, and there is not much the little guy can do about it.

13. a. When I make plans, I am almost certain that I can make them work.

b. It is not always wise to plan too far ahead because many things turn out to- be a matter of good or bad fortune anyhow.

14. a. There are certain people who are just no good. b. There is some good in everybody.

15. a. In my case getting what I want has little or nothing to do with luck. b. Many times we might just as well decide what to do by flipping a coin.

16. a. Who gets to be the boss often depends on who was lucky enough to be in the right place first.

b. Getting people to do the right thing depends upon ability. Luck has little or nothing to do with it.

17. a. As far as world affairs are concerned, most of us are the victims of forces we can neither understand, nor control.

b. By taking an active part in political and social affairs the people can control world events.

18. a. Most people don't realize the extent to which their lives are controlled by accidental happenings.

b. There really is no such thing as "luck."

19. a. One should always be willing to admit mistakes.

b. It is usually best to cover up one's mistakes.

20. a. It is hard to know whether or not a person really likes you.

b. How many friends you have depends upon how nice a person you are.

21. a. In the long run the bad things that happen to us are balanced by the good ones.

b. Most misfortunes are the result of lack of ability, ignorance, laziness, or all three.

22. a. With enough effort we can wipe out political corruption.

b. It is difficult for people to have much control over the things politicians do in office.
23. a. Sometimes I can't understand how teachers arrive at the grades they give. b. There is a direct connection between how hard I study and the grades I get.

24. a. A good leader expects people to decide for themselves what they should do. b. A good leader makes it clear to everybody what their jobs are.

25. a. Many times I feel that I have little influence over the things that happen to me. b. It is impossible for me to believe that chance or luck plays an important role in my life.

26. a. People are lonely because they don't try to be friendly. b. There's not much use in trying too hard to please people, if they like you, they like you.

27. a. There is too much emphasis on athletics in high school. b. Team sports are an excellent way to build character.

28. a. What happens to me is my own doing. b. Sometimes I feel that I don't have enough control over the direction my life is taking.

29. a. Most of the time I can't understand why politicians behave the way they do. b. In the long run the people are responsible for bad government on a national as well as on a local level.

Score one point for each of the following:

2. b, 3.a, 4.a, 5.a, 6.b, 7.b, 9.b, 10.a, 11.a, 12.a, 13.a, 15.a, 16.b, 17.b, 18.b, 20.b, 21. b, 22.a, 23.b, 25.b, 26.a, 28.a, 29.b.

Items 1, 8, 14, 19, 24, and 27 are throwaway items and should be discarded.

A high score = Internal Locus of Control
A low score = External Locus of Control
The 6-item general risk perception (Hunter, 2006) scale—measures general risk perception

1. Drive your car on a freeway near your home, during the day, at 65 MPH in moderate traffic, during heavy rain.

2. Jaywalk (cross in the middle of the block) across a busy downtown street.

3. Climb up a 10-foot ladder to replace an outside light bulb.

4. Take a 2-hour flight in a jet aircraft on a major US air carrier.

5. Drive your car on a freeway near your home, during the day at 65 MPH in moderate traffic.

6. Ride an elevator from the ground floor to the 25th floor of an office building.
The six cyber risk perception items—measures cyber risk perception (CRP)

1. Do not allow your computer to run security updates when it requests to do so.

2. Use the name of someone close to you (including a pet) as your computer password.

3. Open an attachment to an email from an unsecure source.

4. Share your computer password with a co-worker.

5. Insert a USB drive that you found in the parking lot into your computer.

6. Delay password change until forced to do so.
Stanton (2005) et al.’s Taxonomy of Security Risk Behaviors—measures cyber misbehavior (CMB)

Please indicate how often you have engaged in the following behaviors within the past year.

1=Never, 2=Once, 3=Twice, 4=Several times, 5=Monthly, 6=Weekly, 7=Daily

1. I choose relatively simple passwords for my work computer.

2. I have shared my work account user name or password with a friend or coworker.

3. I have installed unauthorized software from the internet onto my work computer without permission from my employer.

4. I have used my social security number as my password.

5. I have written my work password on a piece of paper and left it where others might see it.

6. I have copied work information onto a personal USB drive to do work at home.
The 10-item sensation seeking representation of the Goldberg (1992) markers for the Big-Five factor structure—measures sensation seeking (SSEEK)

Please read each item carefully and then choose an option on the scale.

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

1. Enjoy being reckless.
2. Take risks.
3. Seek danger.
4. Know how to get around the rules.
5. Am willing to try anything once.
6. Seek adventure.
7. Would never go hang-gliding or bungee-jumping.
8. Would never make a high-risk investment.
9. Stick to the rules.
10. Avoid dangerous situations.

The first six items are positively keyed; the last four items are negatively keyed.

For + keyed items, the response “Very Inaccurate” is assigned a value of 1, “Moderately Inaccurate” a value of 2, “Neither Inaccurate nor Accurate” a 3, “Moderately Accurate” a 4, and “Very Accurate” a value of 5.

For – keyed items, the responses receive the opposite values.

Sum the values to obtain the total score.
Experience with Cyber Malfeasance

1. How many years have you regularly used a computer at work?

2. How many hours a week do you use a computer at work?

3. Have you or someone close to you ever been the target of a phishing scam?

4. Have you or someone close to you ever had your information technology compromised?

5. Have you or anyone close to you ever been the victim of any other type of cyber crime?
Demographics

1. What is your age?

2. What is your gender?

3. What is 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

4. How long have you worked at your current job?

5. How many hours a week do you work?
APPENDIX B

Institutional Review Board Approval Letter

Kim Johnson
Psychology
Tampa, FL 33612

RE: Exempt Certification
IRB#: Pro00030814
Title: Cyber Behaviors in the Workplace

Dear Dr. Johnson:

On 5/18/2017, 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.

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.
Table 1. Fit Statistics/Model Comparison: Locus of Control

<table>
<thead>
<tr>
<th>Models</th>
<th>$\chi^2 (df)$</th>
<th>$p$-value</th>
<th>CFI</th>
<th>TLI</th>
<th>SRMR</th>
<th>RMSEA [99%CI]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model 1</td>
<td>14.98 (13)</td>
<td>0.38</td>
<td>0.996</td>
<td>0.995</td>
<td>0.033</td>
<td>0.018 [0.000, 0.071]</td>
</tr>
<tr>
<td>Model 2</td>
<td>96.41 (63)</td>
<td>0.00</td>
<td>0.950</td>
<td>0.938</td>
<td>0.047</td>
<td>0.051 [0.029, 0.070]</td>
</tr>
<tr>
<td>Model 3</td>
<td>23.53 (24)</td>
<td>0.49</td>
<td>1.000</td>
<td>1.002</td>
<td>0.030</td>
<td>0.00 [0.000, 0.055]</td>
</tr>
<tr>
<td>Model 4</td>
<td>186.37 (63)</td>
<td>0.00</td>
<td>0.816</td>
<td>0.772</td>
<td>0.173</td>
<td>0.097 [0.081, 0.114]</td>
</tr>
<tr>
<td>Model 5</td>
<td>95.70 (62)</td>
<td>0.00</td>
<td>0.950</td>
<td>0.937</td>
<td>0.047</td>
<td>0.051 [0.029, 0.071]</td>
</tr>
</tbody>
</table>
Table 2. Fit Statistics/ Model Comparison: Sensation Seeking

<table>
<thead>
<tr>
<th>Models</th>
<th>$\chi^2$ (df)</th>
<th>$p$-value</th>
<th>CFI</th>
<th>TLI</th>
<th>SRMR</th>
<th>RMSEA[99%CI]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model A</td>
<td>439.91 (207)</td>
<td>0.00</td>
<td>0.832</td>
<td>0.813</td>
<td>0.073</td>
<td>0.074 [0.064, 0.083]</td>
</tr>
<tr>
<td>Model B</td>
<td>470.96 (206)</td>
<td>0.00</td>
<td>0.833</td>
<td>0.813</td>
<td>0.073</td>
<td>0.079 [0.069, 0.088]</td>
</tr>
<tr>
<td>Model C</td>
<td>452.05 (207)</td>
<td>0.00</td>
<td>0.823</td>
<td>0.803</td>
<td>0.076</td>
<td>0.076 [0.066, 0.085]</td>
</tr>
<tr>
<td>Model D</td>
<td>478.17 (206)</td>
<td>0.00</td>
<td>0.817</td>
<td>0.795</td>
<td>0.074</td>
<td>0.081 [0.072, 0.091]</td>
</tr>
</tbody>
</table>