Institute for Homeland Security Solutions

Applied research • Focused results

Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies

September 2012

Authors

Maranda McBride, PhD, North Carolina A&T State University

Lemuria Carter, PhD, North Carolina A&T State University

Merrill Warkentin, PhD, Mississippi State University

Prepared for:
Department of Homeland Security
U.S. Department of Homeland Security
Washington, D.C. 20528

www.dhs.gov

Contract No. 3-312-0212782

Prepared by:

RTI International–Institute of Homeland Security Solutions

Research Triangle Park, North Carolina

None of the investigators have any affiliations or financial involvement that conflicts with the material presented in this report.

Suggested citation: McBride, M., Carter, L., and Warkinten, M. (2012). Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cyber Security Policies. (Prepared by RTI International – Institute for Homeland Security Solutions under contract 3-312-0212782.)

(Prepared by RTI International–Institute for Homeland Security Solutions under contract 3-312-0212782)

This report is based on research conducted under the Institute for Homeland Security Solutions (IHSS) under contract to the Department of Homeland Security, Washington, DC. (Contract 3-312-0212782). The findings and conclusions in this document are those of the author(s), who are responsible for its contents; the findings and conclusions do not necessarily represent the views of the Department of Homeland Security. Therefore, no statement in this article should be construed as an official position of the Department of Homeland Security.

Table of Contents

List of Figures

List of Tables

Overview of Research

Strong evidence indicates that insiders (employees) are the major human threat to the security of an organization's information resources; therefore, it is imperative that we understand the factors that promote compliant and noncompliant cybersecurity behaviors. Appropriate cybersecurity designs, especially within the workplace, should be based on an informed deep understanding of insider psychological profiles. Our research is designed to provide such knowledge. In this study, we identify individual personality traits that shape cybersecurity policy violation intentions. We develop and empirically validate a comprehensive model of cybersecurity violation intention that assesses the impact of personality factors, deterrence factors and protection motivation factors on non-compliance among organizational insiders.

This project will be undertaken in five phases. The results of the first two phases are provided in this report. In phase 1, existing empirical research was evaluated to identify key predictors of cybersecurity policy compliance. A comprehensive literature review was conducted to identify personal characteristics that can be used to categorize workplace computer users in the context of cybersecurity compliance factors. Phase 2 entailed the creation of a research model based on the literature review and associated concrete research hypotheses which link the salient antecedent constructs with the dependent variable – "behavioral intention to violate cybersecurity policies." The relationships between these antecedents and several very specific cybersecurity behaviors, such as password selection and changing, was tested using a survey instrument constructed from previously-validated instruments that have been appropriately modified to fit the context of the present study. Additional scales developed were validated systematically following established guidelines. The survey was administered to employees of numerous companies, both large and small, to identify the link between individual differences and the behavioral intention to violate cybersecurity policies. The data collected was used to assess the impact of the individual characteristics identified in Phase 1 on one's behavioral intention to violate cybersecurity policies in the workplace.

Based on participant responses, diverse profiles of cybersecurity users will be proposed. These profiles will be based on psychological and behavioral factors assessed in the survey. In Phase 3, the knowledge gained in previous phases will be utilized to develop differential cybersecurity training protocols that can be used to meet the needs of diverse demographics and personalities. Phases 4 and 5 involve the development and testing of full cybersecurity training programs based on the psychological and behavioral profiles that were identified in Phase 2.

Background

Cybersecurity Policies and Insider Abuse

Maintaining the security of information systems has become a critical objective because of the significant losses that result from the behaviors and actions of insiders (employees). Insider abuse, which occurs when employees violate cybersecurity policies, is frequently identified as the greatest single source of threat to organizational information systems security (Boss et al, 2009; Warkentin & Willison, 2009). The actions and behaviors of employees may be accidental, volitional (but not malicious), or malicious (Willison & Warkentin, 2012).

Recent industry reports confirm that insider abuse is a large and growing concern for organizations. According to a survey of 583 information technology (IT) and IT security practitioners the financial loss from a security breach can be significant (Ponemon, 2011). Forty-one percent of the respondents indicated that the financial impact of these breaches was $500,000 or more. Fifty-two percent of the respondents say the breaches were caused by insider abuse. Another study which was conducted with over 800 IT managers and executives across North America, indicated that 52 percent of respondents were able to by-pass controls put in place to monitor privileged access (Lynch et al., 2012). Virtually half of all respondents indicated that they had accessed electronic information in the organization that was not relevant to their position.

Technical controls are ineffective at preventing motivated insiders from performing various forms of insider abuse, thus organizations employ a range of behavioral controls, including security education, training, and awareness (SETA) campaigns (Peltier, 2005), appeals to protection motivation (Johnson and Warkentin, 2010), and reminders about formal sanctions against information systems (IS) security violations (D'Arcy, et al. 2009). Accordingly, academic research has investigated the success of these efforts, but not in relation to each other (e.g., studies have investigated deterrence (sanctions) or protection motivation theory (PMT), but not both together). Furthermore, we have learned from Shropshire, et al. (2006) that individual differences, such as personality traits, may be responsible for promoting or encouraging "bad behavior" by certain employees. Questions we seek to answer through this research include: Which factors are more important? How do they interact? What can we learn about how various individual employees might react to various points of leverage or various attitude drivers?

Appropriate cybersecurity designs, especially within the workplace, should be based on an informed deep understanding of insider psychological profiles. Our research is designed to provide such knowledge. In this study, we identify some individual personality traits that shape cybersecurity policy violation intentions. We develop and empirically validate a comprehensive model of cybersecurity violation intention that assesses the impact of personality factors,

deterrence factors and protection motivation factors on non-compliance among organizational insiders.

Individual Differences and Cybersecurity Compliance

One individual difference of particular importance is personality type, which is relatively stable over each person's lifetime (Conley, 1985). Though personality differences cannot be altered through intervention, they can be used to establish empirically-validated employee selection and training contingency assignments. In other words, if we can establish statistically significant relationships between individual differences (such as various personality profiles) and policy violation intention motivations, we can establish guidelines for authoring various protection protocols customized to meet the unique needs of diverse employees within the workplace.

A common personality assessment used in IS literature is the "Big Five" personality test (Buchanan et al., 2005; Engelberg & Sjöberg, 2004; Karim et al., 2009; Landers & Lounsbury, 2006; Lim & Benbasat, 2000; Major et al., 2006; Shropshire et al., 2006; Swickert, 2002). The five personality traits, also referred to as OCEAN, are described in Table 1.

Table 1: Big Five Personality Trait Descriptions

Big Five Trait	Trait Description (Zhang, 2006)
O*penness to experience*	"[People scoring high on the openness scale are] characterized by such attributes as open-mindedness, active imagination, preference for variety, and independence of judgment."
C*onscientiousness*	"People [scoring] high on the conscientiousness scale tend to distinguish themselves for their trustworthiness and their sense of purposefulness and of responsibility. They tend to be strong-willed, task-focused, and achievement-oriented."
E*xtraversion*	"People scoring high on the extraversion scale tend to be sociable and assertive, and they prefer to work with other people."
A*greeableness*	"People [scoring] high on the agreeableness scale tend to be tolerant, trusting, accepting, and they value and respect other people's beliefs and conventions."
N*euroticism*	"People [scoring] high on the [neuroticism] scale tend to experience such negative feelings as emotional instability, embarrassment, guilt, pessimism, and low self-esteem"

In addition to personality traits, we also explore the role of sanctions on non-compliance (Boss et al., 2009; D'Arcy et al., 2009). Deterrence theory (Akers, 1990) suggests that individuals will be deterred from performing undesirable behavior (e.g. crime, computer abuse, policy violation) if they perceive that there will be punishments or sanctions which are certain, severe, and swift. However, such deterrence has a differential effect on individuals due to their relative morality and rationality. The effective application of deterrence controls presumes that individuals consider the benefits of a policy violation (e.g. convenience of temporarily leaving a workstation without logging off, selecting a weak password that is easy to remember, or breaking into a database to steal valuable information) and the costs of such violations (perceived sanction certainty, severity, and celerity (swiftness)), and make a rational choice to engage in noncompliant or criminal behavior. Therefore, SETA programs can inform employees about sanctions, but individuals will cognitively process that information in unique ways.

Finally, we also assess the employee's inherent nature to protect himself from threats. Protection motivation theory (PMT) suggests that when individuals perceive that they are more susceptible to security threats (such as malware or hard drive crashes) and when the threats are more severe, they are more likely to adopt a recommended response to the threat (such as scanning for malware or backing up data), as long as the individual employee possesses sufficient self-efficacy and perceived efficacy in the recommended response, both of which can also be influenced (Anderson & Agarwal, 2010; Johnston & Warkentin, 2010).

Project Activities

Initial Survey Design

After completing an extensive literature review, we developed a research model that incorporated the Big Five personality factors as well as PMT and Deterrence Theory factors. The team presented their model to IS professionals at the IFIP Dewald Roode Information Security Workshop in Blacksburg, VA and the Decision Sciences Institute Annual Meeting in Boston, MA. The model was also presented to IS students and professors at Mississippi State University (MSU) and the University of North Carolina – Greensboro (UNCG). Feedback obtained feedback from these sessions were used to modify the theoretical model upon which the survey instrument was based.

The factorial survey approach was used to develop the preliminary survey instrument. The factorial survey approach is a variant of the scenario design and, through the use of scenarios, is able to provide contextual detail to decision making situations and to evenly distribute these details across all participants in the study. Each scenario described a situation in which a company's employee, named Joe, has collected sensitive customer data for his company and wants to take the data home to continue his work. In each scenario, Joe

disregards a mandatory password encryption procedure thus violating a cybersecurity policy. Respondents were asked to estimate the chance that they would duplicate the employee's actions under similar conditions.

The response options in the preliminary survey, ranged from one to five, where five represents strong agreement with engaging in actions similar to those of Joe. Situational factors manipulated as part of each scenario included Joe's perception of threat severity and susceptibility, self-efficacy, response efficacy, sanction severity and certainty, and response cost. The dependent variable in this study is the respondent's self-reported intention to violate a cybersecurity policy as described in each scenario. The Big Five personality traits were assessed using a 100-item 9-point Likert scale (Goldberg, 1992), capturing the distinct factors of openness, conscientiousness, extraversion, agreeableness, and neuroticism.

The preliminary survey instrument was subjected to an expert panel review by subject matter experts and survey design experts at MSU. The expert panel consisted of nine faculty and PhD students with training in instrument development and survey design. Survey items were refined based on the expert panel feedback and a research protocol was submitted to North Carolina Agricultural and Technical State University's (NCAT) Institutional Review Board (IRB) for expedited review. Requested revisions were completed, the protocol was approved, and a pilot test was conducted using paper surveys in December. This survey consisted of 100 items to assess respondents' personality based on the Big Five personality traits (see Appendix A) and four scenarios (see Appendix B for an example). Each scenario had 13 items requiring a response. The first four items were considered manipulation checks to ensure that the respondent paid close attention to the important details of the scenario. These were included because the first two sentences in each scenario were the same, but the wording of the last two sentences differed based upon the level of the situational factors under consideration.

The six situational factors that were manipulated in the study included Self-Efficacy, Response Efficacy, Threat Severity, Threat Vulnerability, Sanction Severity, and Sanction Certainty. Each situational factor had two levels (high and low). The combinations of these levels mathematically resulted in 64 unique versions of the scenario of which each subject assessed only four. These levels are shown in Appendix C. There were two additional situational factors that were not manipulated but were also assessed in the study – Response Cost and Realism. Table 2 provides the anchors for each Big Five personality trait assessed and Table 3 provides definitions for each situational factor.

Table 2: Definitions of Big Five Personality Traits

Trait	Anchor
Openness	consistent/cautious vs. inventive/curious
Conscientiousness	easy-going/careless vs. efficient/organized
Extroversion	solitary/reserved vs. outgoing/energetic
Agreeableness	cold/unkind vs. friendly/compassionate
Neuroticism	secure/confident vs. sensitive/nervous

Table 3: Definitions of Situational Factors

Situational Factor	Definition
Self-Efficacy	Perceived confidence in the ability to comply with cybersecurity policy
Sanction Certainty	Perceived likelihood of being punished if the cybersecurity policy is violated
Sanction Severity	Perceived harshness of the punishment associated with violating cybersecurity policy
Threat Vulnerability	Perceived risk of something negative occurring if cybersecurity policy is violated
Threat Severity	Perceived seriousness of the risk associated with violating cybersecurity policy
Response Efficacy	Perceived effectiveness of cybersecurity policy
Response Cost	Perceived negative consequences associated with complying with cybersecurity policy
Realism	Perceived likelihood that a scenario such as the one presented could occur in the workplace

The paper surveys were administered to 46 business professionals, the majority of whom were enrolled in a professional MBA program at Wake Forest University. Each participant was asked to complete the 100-item Big Five assessment and 4 scenarios.

Paper Pilot Test Results

Out of a total sample size of 184 scenario responses, 126 passed the four manipulations checks designed to determine whether or not the participant paid close attention to the details of the scenarios and 105 passed both the manipulation checks and rated the reality of the scenario at least 3 on a Likert scale from 1 to 5 with 5 being the most realistic.

A mixed model linear analysis was conducted in SPSS. Because of the size of the model, a fractional factorial process was used. The main effects for each situational factor

were assessed first. Then the interactions between each Big 5 trait and situational factor were analyzed. The analysis indicated significant main effects for Threat Severity, Sanction Severity, and Response Cost.

Online Pilot Test

In addition to the paper instrument, the online instrument was constructed and tested by experts in IS and survey design at Mississippi State University. Based on the results of the paper pilot test and feedback from other survey reviewers, modifications were made to the Big Five portion of the survey. The primary modification was that the Big Five assessment was decreased from 100 items to 44 with a Likert scale from 1 to 5 (see Appendix D).

After adding some additional functions to the online survey instrument to increase the number of usable responses, data was collected during a second round of pilot testing. The full online survey used for this test can be accessed using the following link: https://ncat.qualtrics.com/SE/?SID=SV_8G31V1u1h3Zop0w. Out of a total of 684 scenario responses, 481 passed all four manipulation checks and had a reality of 3 or higher. This data was subjected to statistical analysis.

Online Pilot Test Results

A general linear mixed model (GLMM) analysis was conducted in SPSS where the Big Five personality traits were treated as direct determinants of intention (see Figure 1). The significant results of the analysis are shown in the Table 4. (Note: significance was determined by $\alpha \leq 0.05$.) Based upon this analysis, when Sanction Certainty is low or when Response Cost is higher, participants indicated that they were less likely to comply with the cybersecurity policy. In addition, more Open, Conscientious, and Agreeable participants were more likely to comply with the cybersecurity policy. Conversely, more Extroverted and Neurotic participants were more likely to violate the cybersecurity policy.

Another GLMM analysis was conducted in SPSS where the Big Five personality traits were treated as moderating factors to the situational factors (see Figure 2). The significant results of the analysis are shown in Table 5. (Note: significance was determined by $\alpha \leq 0.05$.) Based on the results from the second analysis, when we allow for interactions, Response Cost is no longer significant, but Sanction Severity and Sanction Certainty are both significant. There are also several significant interactions between the personality traits and the base model factors. In addition, Openness, Conscientiousness, and Neuroticism remain significant as direct antecedents.

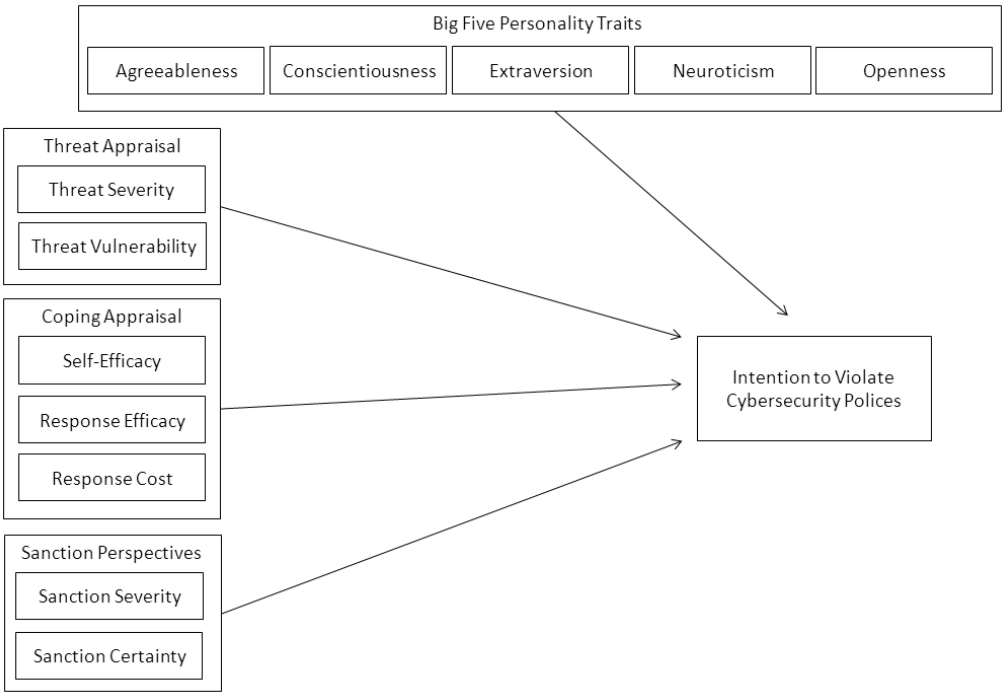


Figure 1: Research Model 1 with Big Five Traits as Direct Determinants of Intention to Violate Cybersecurity Policies

Table 4: Significant Statistical Results for Research Model 1 – Online Pilot Test

Dimension and Level	Coefficient (β)	P-value (α)
Sanction Certainty (Low)	0.151	0.035
Response Cost	0.106	0.054
Openness	-0.151	0.017
Conscientiousness	-0.308	0.000
Extroversion	0.256	0.000
Agreeableness	-0.172	0.014
Neuroticism	0.237	0.000

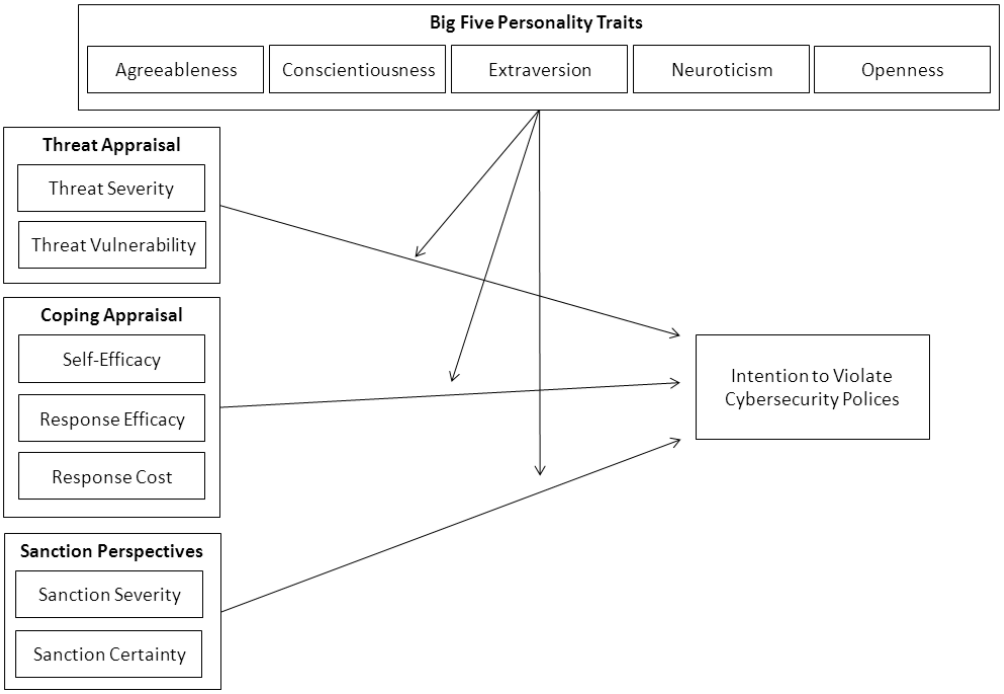


Figure 2: Research Model 2 with Big Five Traits as Moderators of the Situational Factors

Table 5: Significant Statistical Results for Research Model 2 – Online Pilot Test

Dimension and Level	Coefficient (β)	P-value (α)
Sanction Severity (Low)	1.714	0.034
Sanction Certainty (Low)	1.888	0.019
Openness	-0.607	0.083
Conscientiousness	1.515	0.002
Neuroticism	0.587	0.028
Openness*Threat Severity (Low)	0.427	0.001
Conscientiousness* Threat Severity (Low)	-0.449	0.005
Conscientiousness *Response Efficacy (Low)	-0.282	0.090
Conscientiousness * Sanction Severity (Low)	-0.392	0.022
Conscientiousness *Response Cost	-0.321	0.025
Extroversion*Response Efficacy (Low)	0.205	0.087
Extroversion* Sanction Certainty (Low)	0.267	0.025
Agreeableness* Response Efficacy (Low)	0.267	0.082
Agreeableness* Sanction Certainty (Low)	-0.329	0.023
Neuroticism* Sanction Severity (Low)	-0.212	0.031
Neuroticism* Sanction Certainty (Low)	-0.161	0.097

Survey Design Changes

Prior to initiating the field data collection process, several changes were made to the online survey instrument to emphasize the differences between scenarios and to improve the number of usable responses. These changes are listed below.

- Key text was underlined to ensure the subjects notice the differences between scenarios.
- Scenarios were broken into three paragraphs to facilitate readability.
- Each respondent were presented only 3 scenarios instead of 4 to reduce confusion and survey fatigue.
- The penultimate sentence was changed to increase the perceived response cost.
- All Likert scales were changed from 5-point to 7-point to enable a wider spread across the data an increase the ability to detect response differences between conditions.
- Updated survey link: https://ncat.qualtrics.com/SE/?SID=SV_1yOMYb3nK6OCk60.

Field Tests

There were 317 usable observations obtained from an online sample of 150 individuals who met both of the following conditions: 1) have held a job that required the use of a computer and 2) have held a job where employees must follow security procedures. Following a random design factorial survey approach advocated by Rossi and Anderson (1982), participants were asked to read and respond to the online survey that contained three randomly generated hypothetical scenarios, yielding 595 observations at the vignette level, of which 278 were removed due to failures in the manipulation checks and/or the content validity (realism) measure, resulting in 317 usable observations. Based on a power analysis (see Appendix E for explanation), 210 survey responses were needed to achieve the desired statistical power. Ultimately 140 responses from our industry partners, 61 from personal contacts and professional affiliations, and 116 from a Qualtrics panel met the inclusion criteria. Pie graphs illustrating the demographic data of the participants are provided in Appendix F.

Field Test Results

The Big Five data was analyzed using composite scores for each of the five traits. The composite scores were calculated by taking the average score for all positively framed items used to assess each trait. The negatively framed items were dropped from the analysis due to low factor loadings; therefore, 28 items were included in the analysis as opposed to 44. Appendix G provides frequency diagrams for each Big Five factor showing how many individual respondents fell within each 1-point range of the 7-point scale. The composite scores for Behavioral Intent and Realism were calculated using the average score for the three questions used to assess each variable. For Response Cost, only two questions were used to

calculate the composite score since one question was dropped due to low factor loadings. The possible scores for each item ranged from 1 to 7. (Note: The detailed survey validity assessments can be found in Appendix H.) Only responses to scenarios in which all four manipulation checks were answered correctly and the Realism score was 4 or higher were included in the analysis.

Descriptive statistics for the scale data are shown in Table 6. These responses were analyzed using the SPSS general linear mixed model analysis whereby the dependent variable was behavioral intent. The independent variables were the Big Five factors listed in Table 2 and the seven situational factors listed in Table 3. Because of the size of the model, a fractional factorial process was used. Significance was determined by $\alpha \leq 0.05$.

Table 6: Descriptive Statistics

Factor	Mean	Std. Dev.	Minimum	Maximum
Openness	4.85	0.90	2.75	7.00
Conscientiousness	5.92	0.63	3.25	7.00
Extroversion	4.87	1.02	1.60	7.00
Agreeableness	5.50	0.79	2.20	7.00
Neuroticism	3.48	1.15	1.20	6.60
Response Cost	4.65	1.39	1.00	7.00
Realism	5.59	0.71	4.00	7.00
Behavioral Intent	2.31	1.27	1.00	6.00

Initially a general linear mixed model analysis was conducted in SPSS where the Big Five personality traits were treated as direct determinants of intention (refer to Figure 1). The significant results of the analysis are shown in Table 7. Based on these results, the following statements can be made.

- When Self-Efficacy is low, individuals are more likely to violate cybersecurity policies.
- When Threat Vulnerability is low, individuals are more likely to violate cybersecurity policies.
- When Sanction Certainty is low, individuals are more likely to violate cybersecurity policies.
- When Sanction Severity is low, individuals are more likely to violate cybersecurity policies.
- More Open individuals are less likely to violate cybersecurity policies.
- More Extroverted individuals are more likely to violate cybersecurity policies.
- More Neurotic individuals are less likely to violate cybersecurity policies.

Table 7: Statistical Results for Model with Big Five Traits as Direct Determinants of Behavioral Intent

Dimension and Level	Coefficient (β)	P-value (α)
Self-Efficacy (Low)	0.274	0.003
Threat Vulnerability (Low)	0.434	<0.001
Sanction Certainty (Low)	0.250	0.010
Sanction Severity (Low)	0.207	0.032
Openness	-0.140	0.010
Extroversion	0.128	0.011
Neuroticism	-0.166	<0.001

Another general linear mixed model analysis was conducted in SPSS where the Big Five personality traits were treated as moderating factors to the situational factors (refer to Figure 2). The significant results of the analysis are shown in Table 8. Table 9 summarizes these significant effects.

Table 8: Statistical Results for Model with Big Five Traits as Moderating Factors

Dimension and Level	Coefficient (β)	P-value (α)
Threat Severity (Low)	3.895	0.002
Response Efficacy (Low)	-3.753	0.005
Openness	0.532	0.016
Openness*Self-Efficacy (Low)	-0.260	0.033
Neuroticism*Self-Efficacy (Low)	-0.263	0.004
Openness*Threat Severity (Low)	-0.237	0.043
Conscientiousness*Threat Severity (Low)	-0.438	0.013
Extroversion*Threat Severity (Low)	0.220	0.044
Agreeableness*Threat Severity (Low)	-0.280	0.043
Extroversion*Threat Vulnerability (Low)	0.264	0.015
Conscientiousness*Response Efficacy (Low)	0.491	0.004
Agreeableness*Response Efficacy (Low)	0.330	0.018
Openness*Sanction Severity (Low)	0.495	<0.001
Extroversion*Sanction Severity (Low)	-0.589	<0.001
Neuroticism*Sanction Severity (Low)	-0.266	0.004
Agreeableness*Sanction Certainty (Low)	-0.323	0.038
Neuroticism*Sanction Certainty (Low)	0.332	<0.001
Response Cost*Openness	-0.115	0.001
Response Cost*Extroversion	0.076	0.023

Table 9: Effects of Big Five Traits on Deterrence Theory, PMT, and Efficacy Factors

Individuals who are less likely to violate cybersecurity protocol	Individuals who are more likely to violate cybersecurity protocol
• Open individuals with a low sense of Self-Efficacy • Open individuals with a low sense of Threat Severity • Open individuals with a low sense of Response Cost • Conscientious individuals with a low sense of Threat Severity • Extroverted individuals with a low sense of Sanction Severity • Agreeable individuals with a low sense of Self-Efficacy • Agreeable individuals with a low sense of Sanction Severity • Neurotic individuals with a low sense of Self-Efficacy • Neurotic individuals with a low sense of Sanction Severity	• Open individuals in general • Open individuals with a low sense of Sanction Severity • Conscientious individuals with a low sense of Response Efficacy • Extroverted individuals with a low sense of Threat Severity • Extroverted individuals with a low sense of Threat Vulnerability • Extroverted individuals with a low sense of Response Cost • Agreeable individuals with a low sense of Sanction Certainty • Neurotic individuals with a low sense of Sanction Certainty

Discussion

The results of this study confirm that individuals with different personality traits indeed react differently to the same scenarios and imply that the approach we adopt to cybersecurity training must also differentiate between individual employee personality types. Individuals are not the same; employees respond to cybersecurity policies differently. We now have data to show that not only are personality factors a differentiator of cyber security compliance; but also to show that personality factors have an impact on how individuals react to security threats and organizational sanctions. Hence, organizations should adopt a more nuanced approach to cybersecurity instruction that provides training that is appropriate for each individual. Based on our data, we have established that individuals react to cybersecurity threats and deterrents in different ways and that their personality affects the way they approach compliance with cybersecurity policies. Therefore, security education, training and awareness (SETA) programs should reflect these differences and provide appropriate training protocols to each individual trainee. Rather than utilizing a one-size-fits-all training approach, organizations should provide cybersecurity training and other persuasive messages that are customized to address the unique elements of employees' personalities.

Training protocols should be developed that target different types of employees. As indicated in Table 9 there are numerous factors that contribute to one's likelihood to comply with or violate cybersecurity polices. To illustrate the application of these findings, we provide a discussion of one bulleted point from each side of the table. For example, one of the findings from Table 9 indicates that extroverted individuals with a low sense of sanction severity are less likely to violate cyber security policies. Now that we have empirically established this relationship, future scholars can develop a training protocol that is framed in such a way that it will have more impact on individuals with a low sense of sanction severity. For instance, extroverted individuals with a low sense of sanction severity are not motivated by punishments (such as a receiving a negative evaluation or losing their job). Hence, training for these individuals could de-emphasize sanctions as a part of the training program, especially appeals which focus on the severity of sanctions.

With regards to those individuals who are more likely to violate policy, one of our findings indicates that agreeable individuals with a low sense of sanction certainty are more likely to violate cybersecurity policies. Simply being an agreeable individual doesn't necessarily mean that you more or less likely to violate a cybersecurity policy. However, our research indicates that agreeable individuals who feel that sanctions may not be likely are more likely to violate cybersecurity policies even when they are equipped with the knowledge that punishments are likely to be enforced. Hence, training protocols for these individuals might focus on the impact of other situational factors instead of sanctions (since sanction certainty is not an effective motivator for these individuals). They may feel they will not be caught or that punishment is unlikely. Perhaps, training protocols which leverage appeals to threat severity will be more effective.

Based on our findings, we posit that customized training protocol will be more effective at preventing cyber security policy violation than a generic training protocol. These combinations of Big Five personality factors and reactions to deterrents and threats provide us with a path to follow to leverage our understanding of how these factors interact to promote or deter cybersecurity compliance. An organization that doesn't provide this nuanced approach to cybersecurity is less likely to achieve its goal of employee compliance with cyber security policies.

Based on our review of existing cybersecurity studies and the findings of this study, we suggest that there are three levels of cybersecurity training. Ultimately, our goal is to use the findings of this study to develop customized protocols that would support help organizations to achieve level three cybersecurity training.

Three Levels of Cybersecurity Training

Level One – This is the *status quo*. Currently, most organizations provide one training protocol to all employees. The protocol may include a discussion of security threats (if you don't follow this policy you may lose your data) and/or organizational sanctions (if you don't follow this

policy you will be reprimanded). However, this approach does not account for individual differences.

Level Two – A few organizations may utilize a training protocol that leverages the direct effects of personality factors and/or the seven situational factors. For example, a training protocol in an organization where the culture emphasizes the importance of following the rules, may indicate the importance of following the cybersecurity policy and highlight the consequences of noncompliance. This approach may incorporate a few individual differences, but it does not account for the interactions between diverse individual factors.

Level Three – This represents the next step for research on cybersecurity compliance training development. This approach would explore the combined effects of the Personality Factors and/or the seven situational factors. It would take into account how various personality traits interact with individual perceptions of security threats and sanctions. The results of this study, which are presented in Table 9, can be used to develop a set of employee profiles that categorize organizational employees based on their personality types and perceptions of cybersecurity threats and sanctions. In order for organization to implement these customized training elements to organizational employees, individual employees would need to complete a brief questionnaire before beginning a training program that assesses his Big Five personality traits and his perceptions of cybersecurity threats and organizational sanctions. Then, based on his responses and the findings presented in Table 9, a set of customized training protocols could be developed to target diverse profiles of individuals. As a result, each employee would receive cybersecurity training that targets his specific personality traits and unique cybersecurity perceptions. These customized training protocols do not exist yet. Our research study sets the ground work for the development of these protocols. Organizations should develop differential training protocols to leverage the knowledge that we have gained about the combinations of the Big Five personality factors and the perceptions of threats and deterrence.

Summary

The development of policies and programs to improve cybersecurity practices depends largely on our ability to obtain a comprehensive understanding of how individuals perceive cybersecurity threats and on how individuals react to various influences such as sanctions and organizational communications, such as fear appeals. Therefore, the purpose of this study was to collect data from computer users related to how they perceive cybersecurity threats primarily inside the workplace, how they perceive the impact of sanctions, and how other factors may influence their overall cognitive processes in the cybersecurity context. The results of this study confirm that individuals indeed react differently to the same conditions and imply that the approach we adopt to cybersecurity training must also differentiate between individual employee archetypes. The proposed model enables us to better understand human

behavior as it relates to cybersecurity and will lead to the development of practices that will help secure businesses against internal security threats. Papers published over the course of this project are located in Appendix I.

Future Efforts

The next questions we will seek to answer include the following: What other differences aside from personality type should be considered? How do we group employees into categories so that we can efficiently deliver cybersecurity training that is appropriate and effective for each type? What are the specific SETA elements that should be assembled and delivered to each category of employee to be trained? Our study posits that we need to move towards a richer, more nuanced approach to cybersecurity training.

Contact Information

Maranda McBride, PhD
North Carolina A&T State University
1601 E. Market Street
Greensboro, NC 27411
Phone: (336) 285-3359
Email: mcbride@ncat.edu

Lemuria Carter, PhD
North Carolina A&T State University
1601 E. Market Street
Greensboro, NC 27411
Phone: (336) 285-3337
Email: ldcarte@ncat.edu

Merrill Warkentin, PhD
Mississippi State University
P.O. Box 9581
Mississippi State, MS 39762-9581
Phone: (662) 325-1955
Email: m.warkentin@msstate.edu

References

Akers R. (1990). Rational choice, deterrence, and social learning theory in criminology: the path not taken. *The Journal of Criminal Law and Criminology*. 81(3):653–676.

Anderson C, Agarwal R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*. 34(3):613-643.

Bollen, K., and Lennox, R. (1991). Conventional Wisdom on Measurement: A Structural Equation Perspective, *Psychological Bulletin,* 110(2), 305-314.

Boss S, Kirsch LJ, Angermeier I, Shingler RA, Boss W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*. 18:151-64.

Buchanan T, Johnson JA, Goldberg LR. (2005). Implementing a five-factor personality inventory for use on the internet. *European Journal of Psychological Assessment*. 21(2):115-127.

Cohen, P., Cohen, J., Teresi, J., Marchi, M., and Velez, C.N. (1990). Problems in the Measurement Latent Variables in Structural Equations Causal Models, *Applied Psychological Measurement,* 14, 183-196.

Conley JJ. (1985). Longitudinal stability of personality traits: A multitrait-multimethod-multioccasion analysis. *Journal of Personality and Social Psychology*. 49(5):1266-82.

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

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

Edwards, J.R., and Bagozzi, R.P. (2000). On the Nature and Direction of Relationships between Constructs and Measures, *Psychological Methods,* 5(2), 155-174.

Engelberg E, Sjöberg L. (2004). Internet use, social skills, and adjustment. *CyberPsychology & Behavior*. 7(1):41-47.

Fornell, C., Rhee, B.-D., and Yi, Y. (1991). Direct Regression, Reverse Regression, and Covariance Structure Analysis, *Marketing Letters,* 2(3), 309-320.

Goldberg LR. (1992). The development of markers for the Big-Five factor structure. *Psychological Assessment*. 4(1), 26-42.

John OP, Naumann LP, Soto CJ. (2008). Paradigm shift to the integrative big-five trait taxonomy: History, measurement, and conceptual issues. In John OP, Robins RW, Pervin LA editors. *Handbook of personality: Theory and research*. New York: Guilford Press.

Johnston AC, Warkentin M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*. 34(3):549-566.

Karim NSA, Zamzuri NHA, Nor YM. (2009). Exploring the relationship between Internet ethics in university students and the Big Five model of personality. *Computers & Education*. 53(1):86-93.

Landers RN, Lounsbury JW. (2006). An investigation of Big Five and narrow personality traits in relation to Internet usage*. Computers in Human Behavior*. 22(2):283-293.

Lim KH, Benbasat I. (2000). The effect of multimedia on perceived equivocality and perceived usefulness of information systems. *MIS Quarterly*. 24(3):449-471.

Lynch C., Merrill B. and Roberts B. (2012). "2012 Trust, Security & Passwords Survey." Cyber-Ark Software, Inc. Publication Date: June 2012. Accessed August 7, 2012 http://www.websecure.com.au/sites/default/files/2012%20CyberArk%20Trust%20Security%20Password%20Report%20FINAL.pdf

Major DA, Turner JE, Fletcher TD. (2006). Linking proactive personality and the Big Five to motivation to learn and development activity. *Journal of Applied Psychology*. 91(4):927-935.

Peltier TR. (2005). Implementing an information security awareness program. *Information Systems Security*. 14(2): 37-48.

Petter, S., Straub, D., and Rai, A. (2007). Specifying Formative Constructs in Information Systems Research, *MIS Quarterly,* 31(4), 623-656.

Ponemon Institute (2011). Perceptions About Network Security: Survey of IT & IT security practitioners in the U.S. Ponemon Institute© Research Report. Publication Date: June 2011. Accessed August 7, 2012 http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf

Prajapati, B., Dunne, M., and Armstrong, R. (2010). Sample size estimation and statistical power analysis. *Optometry Today*, 16(7).

Roberts, N. and Thatcher, J.B. (2009). Conceptualizing and Testing Formative Constructs: Tutorial and Annotated Example. *The DATA BASE for Advances in Information Systems*, 40(3), 9-30.

Rossi PH, Anderson AB. (1982). The factorial survey approach: An introduction. In Rossi PH, Nock SL, editors. *Measuring social judgments: The factorial survey approach*. Beverly Hills, CA: Sage; p. 15-67.

Shropshire J, Warkentin M, Johnston AC, Schmidt MB. (2006). Personality and IT security: An application of the five-factor model. *Proceedings of the Americas Conference on Information Systems; Acapulco, México*.

Swickert RJ, Hittner JB, Harris JL, Herring JA. (2002). Relationships among Internet use, personality, and social support. *Computers in Human Behavior*. 18(4):437-451.

Warkentin M, Willison R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*.18(2):101-105.

Willison R, Warkentin M. (2012). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*. Forthcoming.

Zhang L. (2006). Thinking styles and the big five personality traits revisited. *Personality and Individual Differences*. 40:1177-1187.

Appendix A

Original Big Five Survey

How Accurately Can You Describe Yourself?

Please use this list of common human traits to describe yourself as accurately as possible. Describe yourself as you see yourself at the present time, not as you wish to be in the future. Describe yourself as you are generally or typically, as compared with other persons you know of the same sex and of roughly your same age.

Before each trait, please write a number indicating how accurately that trait describes you, using the following rating scale:

Inaccurate					Accurate			
Extremely	Very	Quite	Slightly	Neither	Slightly	Quite	Very	Extremely
1	2	3	4	5	6	7	8	9

_____ Active	_____ Extraverted	_____ Negligent	_____ Trustful
_____ Agreeable	_____ Fearful	_____ Nervous	_____ Unadventurous
_____ Anxious	_____ Fretful	_____ Organized	_____ Uncharitable
_____ Artistic	_____ Generous	_____ Philosophical	_____ Uncooperative
_____ Assertive	_____ Haphazard	_____ Pleasant	_____ Uncreative
_____ Bashful	_____ Harsh	_____ Practical	_____ Undemanding
_____ Bold	_____ Helpful	_____ Prompt	_____ Undependable
_____ Bright	_____ High-strung	_____ Quiet	_____ Unemotional
_____ Careful	_____ Imaginative	_____ Relaxed	_____ Unenvious
_____ Careless	_____ Imperceptive	_____ Reserved	_____ Unexcitable
_____ Cold	_____ Imperturbable	_____ Rude	_____ Unimaginative
_____ Complex	_____ Impractical	_____ Self-pitying	_____ Uninquisitive
_____ Conscientious	_____ Inconsistent	_____ Selfish	_____ Unintellectual
_____ Considerate	_____ Inefficient	_____ Shallow	_____ Unintelligent
_____ Cooperative	_____ Inhibited	_____ Shy	_____ Unkind
_____ Creative	_____ Innovative	_____ Simple	_____ Unreflective
_____ Daring	_____ Insecure	_____ Sloppy	_____ Unrestrained
_____ Deep	_____ Intellectual	_____ Steady	_____ Unsophisticated
_____ Demanding	_____ Introspective	_____ Sympathetic	_____ Unsympathetic
_____ Disorganized	_____ Introverted	_____ Systematic	_____ Unsystematic
_____ Distrustful	_____ Irritable	_____ Talkative	_____ Untalkative
_____ Efficient	_____ Jealous	_____ Temperamental	_____ Verbal
_____ Emotional	_____ Kind	_____ Thorough	_____ Vigorous
_____ Energetic	_____ Moody	_____ Timid	_____ Warm
_____ Envious	_____ Neat	_____ Touchy	_____ Withdrawn

Appendix B

Sample Scenario

Joe has just collected sensitive customer data for his company, and he wants to take that data home to continue his work. He knows his company requires that he request a password to be issued and applied to all data before taking it out of the office on a USB drive so that it cannot be accessed by an unauthorized individual. Joe has completed the password request procedure before, so he is confident he can do it again easily. Joe believes that without the password, it is not likely that unauthorized people will see the data, but if they do, nothing bad will happen. Joe believes that the password procedure is effective and prevents unauthorized people from seeing the data. Regardless, the password procedure takes several minutes, and he needs to leave now, so he skips the procedure. Joe believes his chances of being caught are low, but if caught, the punishment would be minimal.

Please select an answer for the following items as they relate to the scenario.

How confident was Joe about his ability to complete the password request procedure?

a. He was confident he could do it again easily.
b. He was not confident he could do it again easily.

What did Joe believe about the threat of other people seeing the data?

a. He believed it was not likely they would see the data, but if they did, nothing bad would happen.
b. He believed it was not likely they would see the data, but if they did, they may alter or misuse it.
c. He believed it was likely they would see the data, but if they did, nothing bad would happen.
d. He believed it was likely they would see the data, and if they did, they may alter or misuse it.

What did Joe believe about the effectiveness of the password procedure?

a. He believes that the password procedure is effective and prevents unauthorized people from seeing the data.
b. He believes that the password procedure is not effective and does not prevent unauthorized people from seeing the data.

What did Joe think about the punishment for his actions?

a. Joe thought that it was unlikely he would be punished, and if so, the punishment would not be severe.
b. Joe thought that it was unlikely he would be punished, but if he was, the punishment would be severe.
c. Joe thought that it was likely he would be punished, but the punishment would not be severe.
d. Joe thought that it was likely he would be punished, and the punishment would be severe.

	SD	D	N	A	SA
In this situation, I would do the same as Joe.	1	2	3	4	5
The password request procedure takes a long time.	1	2	3	4	5
The above scenario is a realistic one.	1	2	3	4	5
If I were Joe, I would have also skipped the procedure.	1	2	3	4	5
The password procedure does not take long.	1	2	3	4	5
I could imagine a similar scenario taking place at work.	1	2	3	4	5
I think I would do what Joe did if this happened to me.	1	2	3	4	5
The situation could occur at work.	1	2	3	4	5
The password procedure will take too much time.	1	2	3	4	5

Note: SD = Strongly disagree, D = Disagree, N = Neither agree nor disagree, A = Agree, SA = Strongly agree

Appendix C

Constructs Manipulated in the Scenarios

Below are the statements associated with the various levels of each of the situational factors assessed. The levels are shown in parentheses.

Self-Efficacy Levels

- Joe has completed the password request procedure before, but he is not confident he can do it again easily. (low)
- Joe has completed the password request procedure before, so he is confident he can do it again easily. (high)

Threat Susceptibility and Severity

- Joe believes that, without the password, it is not likely that unauthorized people will see the data, but if they do, nothing bad will happen. (low/low)
- Joe believes that, without the password, it is not likely that unauthorized people will see the data, but if they do, they may alter or misuse it. (low/high)
- Joe believes that, without the password, it is likely that unauthorized people will see the data, but if they do, nothing bad will happen. (high/low)
- Joe believes that, without the password, it is likely that unauthorized people will see the data and if they do, they may alter or misuse it. (high/high)

Sanction Certainty and Severity

- Joe believes his chances of being caught are low, but if caught, the punishment would be minimal. (low/low)
- Joe believes his chances of being caught are low, but if caught, the punishment would be severe. (low/high)
- Joe believes his chances of being caught are high, and if caught, the punishment would be minimal. (high/low)
- Joe believes his chances of being caught are high, and if caught, the punishment would be severe. (high/high)

Response Efficacy

- Joe believes that the password procedure is not effective and does not prevent unauthorized people from seeing the data. (low)
- Joe believes that the password procedure is effective and prevents unauthorized people from seeing the data. (high)

Appendix D

Modified Big Five Survey

HOW I AM IN GENERAL

Here are a number of characteristics that may or may not apply to you. For example, do you agree that you are someone who likes to spend time with others? Please indicate the extent to which you agree or disagree with each statement.

I am someone who…	1-Disagree Strongly	2-Disagree a Little	3-Neither agree nor disagree	4-Agree a little	5-Agree Strongly
Is talkative					
Tends to find fault with others					
Does a thorough job					
Is depressed, blue					
Is original, comes up with new ideas					
Is reserved					
Is helpful and unselfish with others					
Can be somewhat careless					
Is relaxed, handles stress well					
Is curious about many different things					
Is full of energy					
Starts quarrels with others					
Is a reliable worker					
Can be tense					
Is ingenious, a deep thinker					
Generates a lot of enthusiasm					
Has a forgiving nature					
Tends to be disorganized					
Worries a lot					
Has an active imagination					
Tends to be quiet					
Is generally trusting					
Tends to be lazy					
Is emotionally stable, not easily upset					
Is inventive					
Has an assertive personality					
Can be cold and aloof					
Perseveres until the task is finished					
Can be moody					
Values artistic, aesthetic experiences					
Is sometimes shy, inhibited					
Is considerate and kind to almost everyone					
Does things efficiently					
Remains calm in tense situations					
Prefers work that is routine					
Is outgoing, sociable					
Is sometimes rude to others					
Makes plans and follows through with them					
Gets nervous easily					
Likes to reflect, play with ideas					
Has few artistic interests					
Likes to cooperate with others					
Is easily distracted					
Is sophisticated in art, music, or literature					

Appendix E

Statistical Power Analysis

Using the *a prior* power analysis approach (utilizing the G*Power 3 software) described in Prajapati, Dunne, and Armstrong (2010), to a detect an effect size of 0.25 with a power of 0.95 (alpha = 0.05), with 5 covariates and with each factor having no more than two levels, we will need **a minimum of 210 observations**.

F tests - ANCOVA: Fixed effects, main effects and interactions

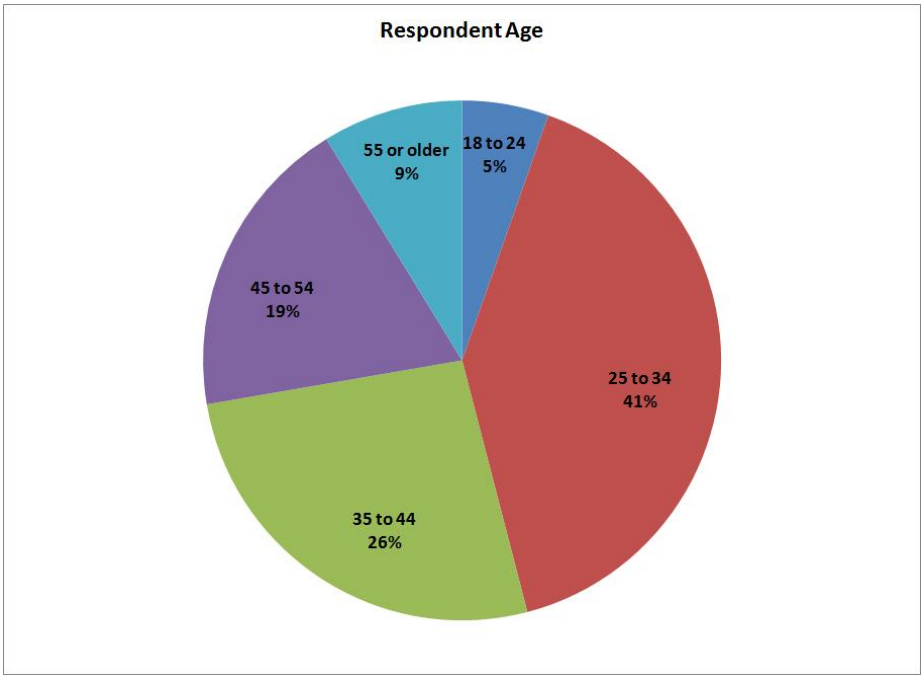
Analysis: A priori: Compute required sample size

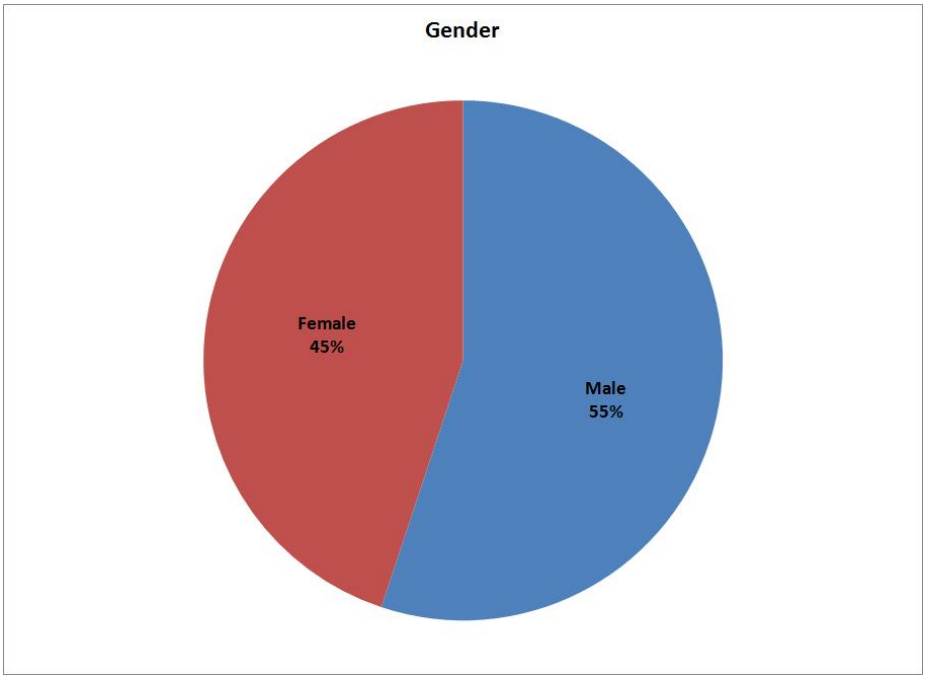
Input:
Effect size f = 0.25
α err prob = 0.05
Power (1-β err prob) = 0.95
Numerator df = 1
Number of groups = 4
Number of covariates = 5

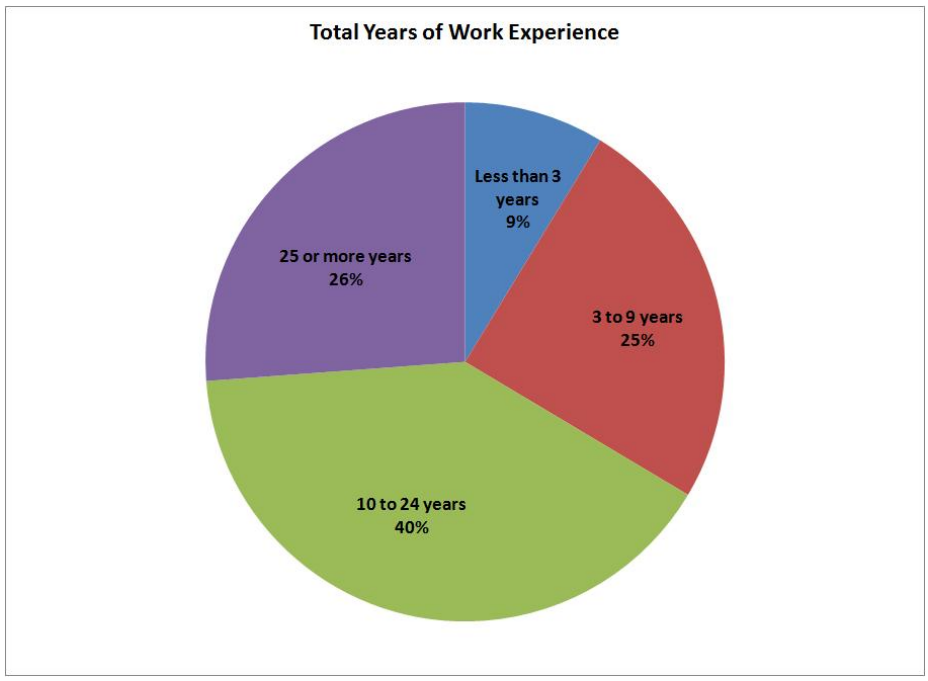
Output: Noncentrality parameter λ = 13.1250000
Critical F = 3.8881392
Denominator df = 201
Total sample size = 210
Actual power = 0.9500684

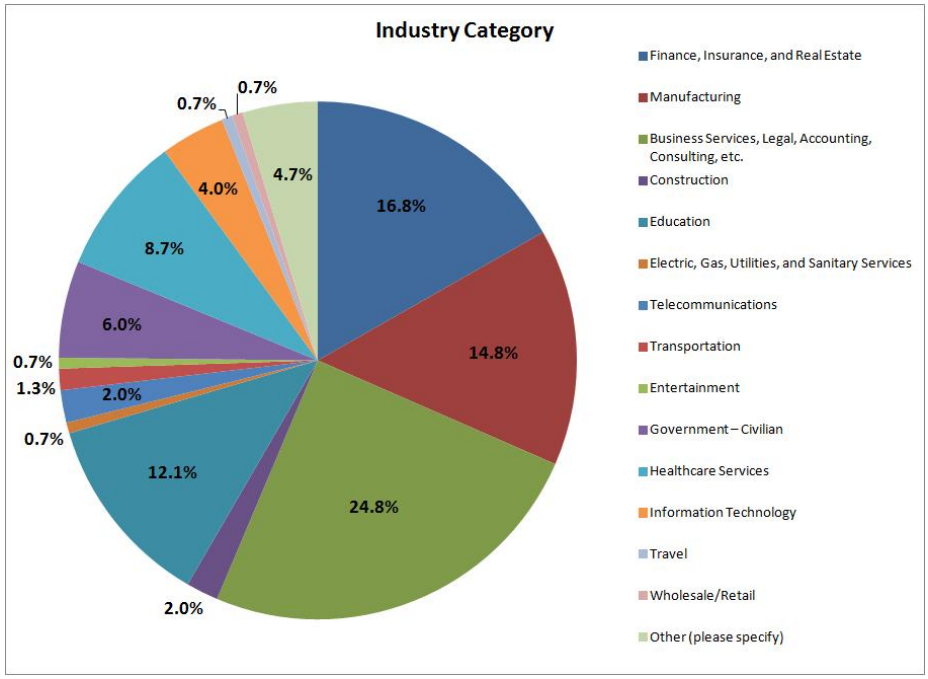
Appendix F

Respondent Demographics



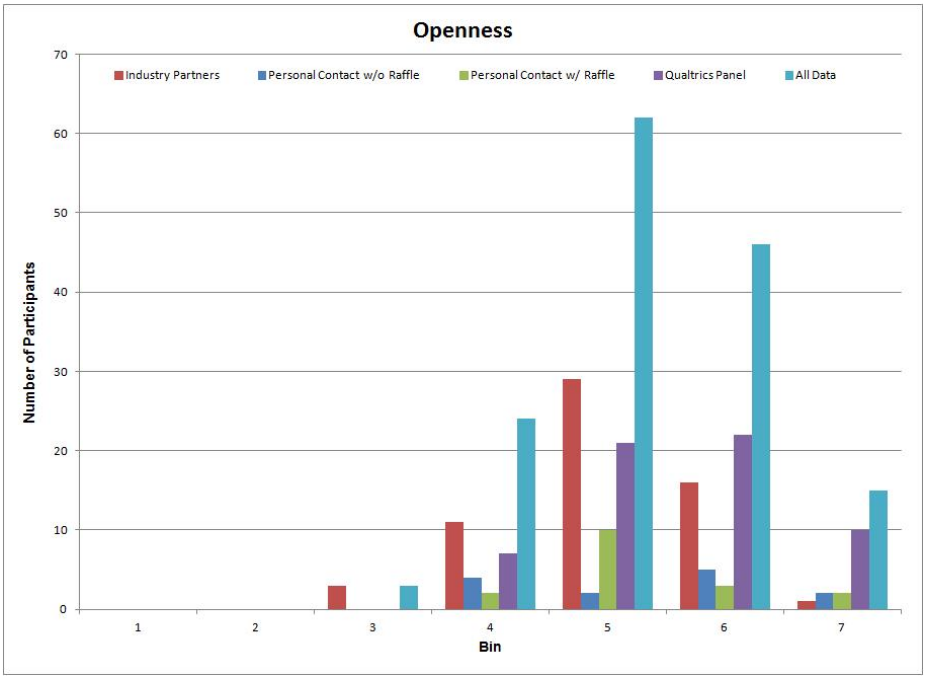


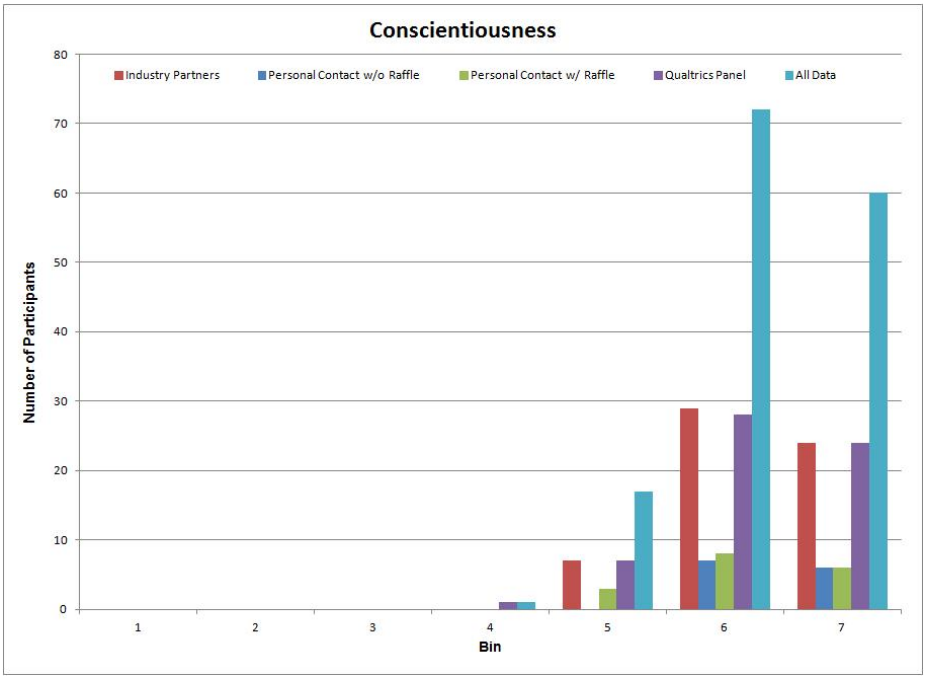

Total Years of Work Experience
Less than 3 years 9%
3 to 9 years 25%
10 to 24 years 40%
25 or more years 26%

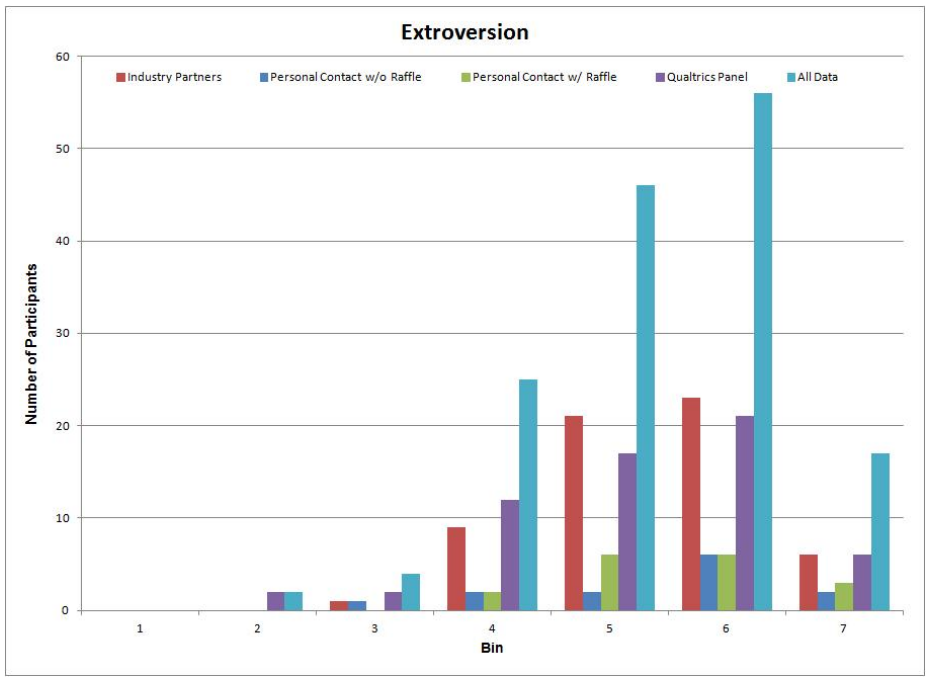

Industry Category
16.8%
14.8%
24.8%
2.0%
12.1%
0.7%
2.0%
1.3%
0.7%
6.0%
8.7%
4.0%
0.7%
0.7%
4.7%
Finance, Insurance, and Real Estate
Manufacturing
Business Services, Legal, Accounting, Consulting, etc.
Construction
Education
Electric, Gas, Utilities, and Sanitary Services
Telecommunications
Transportation
Entertainment
Government – Civilian
Healthcare Services
Information Technology
Travel
Wholesale/Retail
Other (please specify)

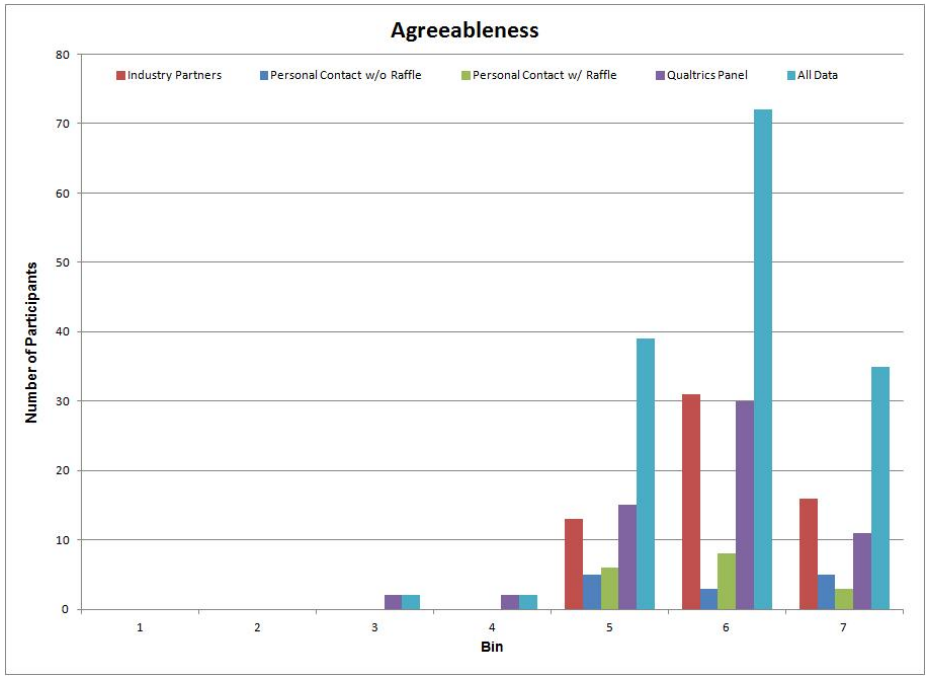
Appendix G

Big Five Trait Frequency Diagrams






Extroversion
Industry Partners
Personal Contact w/o Raffle
Personal Contact w/ Raffle
Qualtrics Panel
All Data
Number of Participants
Bin
0
10
20
30
40
50
60
1
2
3
4
5
6
7


Agreeableness
Industry Partners
Personal Contact w/o Raffle
Personal Contact w/ Raffle
Qualtrics Panel
All Data
Number of Participants
Bin
0
10
20
30
40
50
60
70
80
1
2
3
4
5
6
7

Appendix H

Validity Analysis Results

Step 1: Conduct a Principle Component Analysis

(According to Bollen and Lennox (1991) you may choose to keep nonsignificant measures)

Rotated Component Matrix[a]

	Component						
	1	2	3	4	5	6	7
O1_B5-5	**.675**	.063	.100	.013	-.099	.456	-.033
O2_B5-10	**.561**	.132	.115	.049	-.176	-.282	.066
O3_B5-15	**.513**	-.136	-.179	.061	.171	.314	-.046
O4_B5-20	**.660**	.193	-.129	-.063	.153	-.040	.117
O5_B5-25	**.744**	.055	-.129	.108	-.254	.194	-.060
O6_B5-30	**.657**	.046	.182	-.059	.098	-.209	.069
O7_B5-40	**.761**	.052	.147	-.060	-.067	.001	.050
O8_B5-44	**.453**	.290	-.152	-.052	.082	-.064	.009
C1_B5-3	-.076	.348	-.051	-.046	.045	**.371**	.124
C2_B5-13	.014	.195	.381	-.033	.041	**.495**	.273
C3_B5-28	.080	.032	.054	.080	-.052	**.722**	-.131
C4_B5-33	-.046	-.003	.039	.034	-.132	**.782**	-.013
C5_B5-38	.000	.082	.050	-.109	-.078	**.715**	-.185
E1_B5-1	-.002	**.828**	.102	.056	.070	.018	.031
E2_B5-11	.254	**.648**	.101	-.073	-.314	-.054	-.198
E3_B5-16	.436	**.622**	.091	.013	-.096	.175	-.024
E4_B5-26	.222	**.665**	-.346	.091	-.187	.153	-.068
E5_B5-36	.090	**.850**	.138	.066	-.087	.059	-.061
A1_B5-7	.196	.158	**.612**	.153	.075	.140	-.045
A2_B5-17	.040	-.047	**.697**	.074	-.066	-.115	-.049
A3_B5-22	-.050	-.036	**.604**	-.086	-.227	-.058	-.250
A4_B5-32	-.049	-.006	**.782**	.025	-.041	.146	.015
A5_B5-42	-.022	.059	**.730**	-.023	.042	.079	.066
N1_B5-4	.060	-.347	-.017	.106	**.691**	.017	-.096
N2_B5-14	.061	.111	-.219	-.160	**.710**	-.028	.142
N3_B5-19	-.082	-.078	-.007	-.147	**.786**	-.085	-.150
N4_B5-29	.249	-.168	-.362	-.099	**.529**	-.208	-.031
N5_B5-39	-.212	-.002	.215	-.115	**.726**	-.068	-.173
RCST1	-.005	-.054	.011	-.075	-.089	-.110	**.861**
RCST2	.050	-.051	-.059	-.034	-.101	-.090	**.847**
RCST3	.096	-.024	-.066	.108	-.039	-.004	**.797**
BINT1	.010	.028	.062	**.947**	-.053	.007	-.010
BINT2	-.043	.004	.035	**.948**	-.166	-.017	.017
BINT3	-.027	.061	.034	**.950**	-.099	-.012	.004

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 7 iterations.

Summary of Step 1 Results: This test is used to assess construct validity. Conscientious 1 (C1) does not meet the standard .4 criteria. However, Bollen and Lennox (1991) posit that you may choose to keep nonsignificant measures if they contribute conceptually to the construct. Although statistical results should be considered, conceptual reasoning carries more weight than statistical outcomes when deciding to keep or drop formative constructs (Cohen et al. 1990; Edwards and Bagozzi 2000; Fornell et al. 1991; Petter et al. 2007). Other than Conscientious1(C1), all other items were statistically significant.

Step 2: Test for Multicollinearity
(VIF should be less than 10)

```
REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA COLLIN TOL
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT BINT
  /METHOD=ENTER O C E A N RCST.
```

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.218[a]	.047	.029	1.2500

a. Predictors: (Constant), RCST, E, A, N, C, O

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	24.071	6	4.012	2.568	.019[b]
	Residual	484.340	310	1.562		
	Total	508.412	316			

a. Dependent Variable: BINT

b. Predictors: (Constant), RCST, E, A, N, C, O

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	4.248	.975		4.358	.000		
	O	-.125	.086	-.089	-1.463	.144	.839	1.191
	C	-.151	.120	-.075	-1.263	.208	.870	1.149
	E	.077	.079	.062	.973	.331	.762	1.313
	A	-.016	.094	-.010	-.166	.868	.904	1.106
	N	-.208	.065	-.189	-3.193	.002	.877	1.140
	RCST	.000	.052	.000	.003	.998	.953	1.050

a. Dependent Variable: BINT

Summary of Step 2 Results: This test evaluates the reliability of the constructs. Multicollinearity is not an issue in this data set. The VIF for all variables is less than 10. The items also pass the more stringent test: VIF < 3.3 (Diamontopoulous and Siguaw 2006).

Step 3: Analyze Formative Constructs (conducted using component-based SEM in Smart PLS[1])

(Item weights should be significant)

Outer Weights (Mean, STDEV, T-Values)

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	Standard Error (STERR)	T Statistics (|O/STERR|)	Significant*
A1_B5-7 -> Agreeable	0.818433	0.634819	0.356360	0.356360	**2.296645**	**Yes**
A2_B5-17 -> Agreeable	0.257633	0.248795	0.348863	0.348863	0.738492	No
A3_B5-22 -> Agreeable	-0.167609	-0.144043	0.353257	0.353257	0.474466	No
A4_B5-32 -> Agreeable	0.132711	0.065151	0.360527	0.360527	0.368103	No
A5_B5-42 -> Agreeable	0.059356	0.079495	0.357939	0.357939	**0.165828**	**Yes**
C1_B5-3 -> Concientious	-0.125598	0.060798	0.321609	0.321609	0.390530	No
C2_B5-13 -> Concientious	-0.240534	0.063382	0.427901	0.427901	0.562126	No

[1] Cases with missing values were removed (n=248)

* If T> 1.960, then p < .05, If T> 2.576, then p < .01, If T> 3.291 then p < .001,

C3_B5-28 -> Concientious	0.961961	0.073969	0.784031	0.784031	1.226943	No
C4_B5-33 -> Concientious	0.262196	0.145145	0.423667	0.423667	0.618872	No
C5_B5-38 -> Concientious	-0.924334	0.030827	0.770002	0.770002	1.200430	No
E1_B5-1 -> Extravert	-0.196783	-0.089458	0.404433	0.404433	0.486564	No
E2_B5-11 -> Extravert	-0.244462	-0.108337	0.417855	0.417855	0.585039	No
E3_B5-16 -> Extravert	-0.346508	-0.266971	0.454558	0.454558	0.762295	No
E4_B5-26 -> Extravert	0.347842	0.185017	0.421565	0.421565	0.825120	No
E5_B5-36 -> Extravert	1.135294	0.862997	0.491018	0.491018	**2.312123**	**Yes**
N1_B5-4 -> Neurotic	-0.356802	-0.299312	0.256073	0.256073	1.393358	No
N2_B5-14 -> Neurotic	0.769122	0.668565	0.270178	0.270178	**2.846726**	**Yes**
N3_B5-19 -> Neurotic	0.200890	0.201643	0.363196	0.363196	0.553119	No
N4_B5-29 -> Neurotic	0.272137	0.242439	0.263432	0.263432	1.033041	No
N5_B5-39 -> Neurotic	0.101142	0.070170	0.298743	0.298743	0.338560	No
O1_B5-5 -> Openess	0.313786	0.198001	0.369551	0.369551	0.849101	No
O2_B5-10 -> Openess	-0.650521	-0.236565	0.505622	0.505622	1.286575	No
O3_B5-15 -> Openess	0.124163	0.109493	0.239986	0.239986	0.517375	No
O4_B5-20 -> Openess	0.759036	0.300881	0.573530	0.573530	1.323446	No
O5_B5-25 -> Openess	-0.839111	-0.419201	0.717408	0.717408	1.169642	No
O6_B5-30 -> Openess	0.185555	0.098558	0.273116	0.273116	0.679401	No
O7_B5-40 -> Openess	0.222668	0.131857	0.293390	0.293390	0.758948	No
O8_B5-44 -> Openess	0.205112	0.131695	0.305020	0.305020	0.672457	No

Summary of Step 3 Results: This test measures the contribution of each formative indicator to the variance of the latent variable. These indicator weights are evidence of construct validity (Petter et al. 2007). Significant item weights indicate that an item explains a significant percent of the variance in the formative construct (Roberts and Thatcher 2009). Only four of the twenty items are significant. However, Bollen and Lennox (1991) posit that you may choose to keep nonsignificant measures if they contribute conceptually to the construct. Although statistical results should be considered, conceptual reasoning carries more weight than statistical outcomes when deciding to keep or drop formative constructs (Cohen et al. 1990; Edwards and Bagozzi 2000; Fornell et al. 1991; Petter et al. 2007).

Reflective Constructs

Initial Results

Overview

	AVE	Composite Reliability	R Square	Cronbachs Alpha
Agreeable				
Behavior Intent	0.923382	0.973084	0.165474	0.958628
Concientious				
Extravert				
Neurotic				
Openess				
ResponseCost	**0.455549**	0.664173		0.836487

Cross Loadings

	Response Cost	Behavior Intent
RCST1	0.813719	
RCST2	0.824048	
RCST3	**0.159541**	
BINT1		0.949339
BINT2		0.964783
BINT3		0.968553

Summary of Initial Results: The AVE of ResponseCost is below the standard .50 threshold and RCST3 does not load properly. Hence, I removed RCST3 and reran the analysis.

2nd Round Results (Dropped RCST3)

Overview

	AVE	Composite Reliability	Cronbachs Alpha
Agreeable			
Behavior Intent	0.923335	0.973067	0.958628
Concientious			
Extravert			
Neurotic			
Openess			
ResponseCost	0.871820	0.931518	0.853276

Cross Loadings

	Response Cost	Behavior Intent
RCST1	0.939975	
RCST2	0.927409	
BINT1		0.948844
BINT2		0.965090
BINT3		0.968661

Summary of 2nd Round Results: After removing RCST3, the AVE of ResponseCost passed the .50 test. This indicates that our items display convergent validity. To test discriminant validity (and provide additional support for convergent validity) we conducted a confirmatory factor analysis. All items loaded properly (higher on the intended construct than on other constructs). The Chronbach's Alpha value is higher than the .70 cut-off, indicating that the items are reliable. In summary, our reflective measures are reliable, convergent and discriminant.

Appendix I

Project-Related Research Papers

Completed Papers Attached

- Warkentin, M., Carter, L., and McBride, M. (2011). "Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies." *Proceedings of the IFIP Dewald Roode Information Security Workshop*.

- Warkentin, M., McBride, M., Carter, L., and Johnston, A. (2012). "The role of individual characteristics on insider abuse intentions." *Proceedings of the 18th Americas Conference on Information Systems*.

Paper Under Review

- Warkentin, M., McBride, M., Carter, L., and Johnston, A. (under review). "The impact of personality on employee information security violations." Submitted to *Computers and Security*.