RESEARCH BRIEF

Institute for Homeland Security Solutions
Applied research • Focused results

September 2012

The Role of Situational Factors and Personality on Cybersecurity Policy Violation

Project Leads

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

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

Merrill Warkentin, PhD, Mississippi State University

Statement of Problem

Maintaining the security of information systems has become a critical objective because of the very 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 IT 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, Shropshire, et al. (2006) posit 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: behavioral controls, personality traits, or both? How do they interact? How do various individual employees react to various points of leverage or to diverse 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. Cybersecurity policy violation intention refers to one's willingness to ignore an organization's cyber security protocol. This concept is rooted in the theory of reasoned action (TRA) which posits that a person's attitudes and beliefs influence his intentions and these intentions in turn influence a person's action (Fishbein and Ajzen 1975). 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 to behavioral research 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-tested 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.

One of the common personality assessments used in information systems (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, measured in this test 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).

Methodology

A factorial survey approach was utilized to investigate the research questions presented in this study. 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. We obtained 317 usable observations 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 an 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. 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. Each of the 64 versions of the scenario embedded a different set of independent variable levels, as described below. (A sample scenario is provided in the appendix.)

After reading 3 out of 64 possible scenarios in which 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 ranged from one to seven, where seven represents strong agreement with engaging in actions similar to those of Joe. Situational factors manipulated as part of each scenario include 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 44-item 7-point Likert scale (John et al. 2008), capturing the distinct factors of openness, conscientiousness, extraversion, agreeableness, and neuroticism.

Data Analysis and Results

The data were analyzed using the SPSS general linear mixed model (GLMM) analysis whereby the dependent variable was Behavioral Intent. The independent variables were the Big Five factors and the seven situational factors. Significance was determined by $\alpha \leq 0.05$. We analyzed the data in two phases. In phase one, we tested the direct effects of the Big Five factors and the seven situational factors. In phase two, we explored how the Big Five factors moderate the seven situational factors.

Phase One: Direct Effects

Based on the analysis conducted in which the Big Five personality traits were treated as direct determinants of intention, 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 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.

Phase Two: Moderating Effects of the Big Five

A second analysis was conducted in which the Big Five personality traits were treated as moderating factors to the relationships between the situational factors and intention. Based on the results, conditional effects were found for Response Efficacy, Threat Severity, and Openness. The following statements can be made based on these results:

- When Threat Severity is low, individuals are more likely to violate cybersecurity policies.
- When Response Efficacy is low, individuals are less likely to violate cybersecurity policies.
- More Open individuals are more likely to violate cybersecurity policies.

In addition, several of the Big Five personality traits had moderating effects on the situational factors. Table 2 provides a summary of the significant effects.

Table 2: Effects of Big Five Traits on Deterrence Theory, PMT, and Efficacy Factors

Individuals who are <u>less</u> likely to violate cybersecurity policies	Individuals who are <u>more</u> likely to violate cybersecurity policies
• 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

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 2, 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 2 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 regard 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 2, 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 2, 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.

Conclusions

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 formal sanctions 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 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. 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?

This study represents an initial step to integrate the impact of the Big Five factors with perceptions of threats and sanctions to see how they work together to promote cybersecurity compliance. However, additional research is needed to develop the appropriate set of training protocols and the appropriate framing for each employee profile. The purpose of this study is to establish a foundation for which these protocols can be developed. This study highlights the need for future research to develop customized training protocols that incorporate the interrelations between the Big Five personality factors and individual perceptions of security threats and organizational sanctions. To date, most studies on cybersecurity training utilize standardized training metrics. 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
E-mail: mcbride@ncat.edu

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

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

Maranda McBride, PhD, is an Associate Professor of Management at North Carolina Agricultural &Technical State University (NCA&T). Her research interests include human-computer interaction, decision support display design and auditory display design.

Lemuria Carter, PhD, is an Associate Professor of Accounting at NCA&T. Her research interests include technology adoption, electronic government and cybersecurity.

Merrill Warkentin, PhD, is a Professor of Information Systems at Mississippi State University. His research interests include IS security, electronic collaboration, and electronic commerce/electronic government.

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.

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. 18:151-164.

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.

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.

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

Fishbein, M. & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley.

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.

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

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. 40:1177-11187.

Appendix
Sample Scenario

(manipulations underlined)*

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 works well, and will keep 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.

* Note: Each underlined manipulation is one of several levels for that variable. For example, instead of "chances of being caught are low" – other versions of this scenario say "chances of being caught are high." There are 64 unique combinations of each embedded variable.