The Role of Individual Characteristics on Insider Abuse Intentions

Merrill Warkentin
Mgmt & Information Systems, Mississippi State University, Mississippi State, MS, United States., m.warkentin@msstate.edu

Maranda McBride
North Carolina A&T State University, Greensboro, NC, United States., mcbride@ncat.edu

Lemuria Carter
School of Business and Economics, North Carolina A&T State University, Greensboro, NC, United States., Ldcarte2@ncat.edu

Allen Johnston
University of Alabama Birmingham, Birmingham, AL, United States., ajohnston@uab.edu

Follow this and additional works at: http://aisel.aisnet.org/amcis2012

Recommended Citation
Warkentin, Merrill; McBride, Maranda; Carter, Lemuria; and Johnston, Allen, "The Role of Individual Characteristics on Insider Abuse Intentions" (2012). AMCIS 2012 Proceedings. 28.
http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/28

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2012 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
The Role of Individual Characteristics on Insider Abuse Intentions

Merrill Warkentin  
Mississippi State University  
m.warkentin@msstate.edu  

Maranda McBride  
North Carolina A&T University  
mcbride@ncat.edu  

Lemuria Carter  
North Carolina A&T University  
lcarte2@ncat.edu  

Allen C. Johnston  
University of Alabama Birmingham  
ajohnston@uab.edu

ABSTRACT

Insiders represent a major threat to the security of an organization’s information resources (Warkentin & Willison, 2009; Stanton et al., 2005). Previous research has explored the role of protection motivation or of deterrence in promoting compliant behavior, but these factors have not been studied together. Furthermore, other individual differences, such as the Big Five personality factors may serve as critical influences on cybersecurity compliance. In this study we use a factorial survey approach to identify key components of secure insider behavior. We obtained 201 observations from a diverse sample of employees. The results of this effort will enable us to develop psychological profiles of individual employees so that we may create personalized cybersecurity training protocols that meet the unique needs of each employee profile, appealing to the proper set of motivations for each. Findings of the present study are presented, and the long-term project goal is discussed.

Keywords: Cybersecurity Policy Violation, Protection Motivation Theory, General Deterrence Theory, Personality.

Note: This study is being funded in part by a grant from the Institute of Homeland Security Solutions (IHSS) as part of their Cyber Security Test Bed project. IHSS is a federally funded collaborative initiative which coordinates its research activities with the U.S. Department of Homeland Security’s Human Factors/Behavioral Sciences Division.

INTRODUCTION

Maintaining the security of information systems has become a critical objective because of the very significant losses that result from the intentional, and sometimes malicious, behaviors and actions of insiders (employees). Recent industry reports confirm academic reports that insider abuse is a large and growing concern for organizations, especially during these recessionary times when disgruntled workers engage in various improper acts. 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 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. (Studies have investigated deterrence (sanctions) or protection motivation theory (PMT), but not both together.) Furthermore, we have learned (from Shropshire, et al., 2006, and others) that individual differences, such as personality traits, may be responsible for promoting or encouraging “bad behavior” by certain employees. Which is 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?

Insider abuse, which occurs when employees violate cybersecurity policies, is frequently identified as the greatest single source of threat to organizational information systems security (Warkentin & Willison, 2009; Boss et al, 2009). The actions and behaviors of employees may be accidental, volitional (but not malicious), or malicious (Willison & Warkentin, 2012). According to the results of a recent survey administered to 443 information security and information technology professionals, “twenty-five percent of respondents felt that over 60 percent of their organizations’ financial losses were due to non-malicious actions by insiders (Richardson, 2009).” Forty-three percent of respondents stated that “at least some of their losses were attributable to malicious insiders (Richardson, 2009).” Insiders not only have access to the information and applications (i.e., they are behind the firewall with valid usernames and passwords), they also have intimate knowledge about...
organizational procedures and weaknesses which makes employees supremely situated to take advantage of security vulnerabilities.

The existing literature identifies numerous factors that encourage individuals to either comply with or violate cybersecurity policies (Dhillon and Backhouse 2000). Straub and Welke (1998) established the Security Action Cycle, which identifies the sequential roles of deterrence, prevention, detection, and remediation in minimizing insider abuse. This framework has formed the foundation of a rich stream of subsequent research and has been augmented by the Extended Security Action Cycle (Willison & Warkentin, 2010; 2012). In this framework, organizations can look even further back in time to identify factors that may motivate individual employees to commit acts of internal computer abuse, such as disgruntlement resulting from perceived organizational injustice (Willison & Warkentin, 2010), and the techniques of neutralization (Siponen & Vance, 2010). It has also been shown that, in considering potential acts, some individuals are more responsive to their sense of morality (Siponen & Vance, 2010) and other individuals are more likely to engage in a somewhat rational assessment of the relative benefits and costs of policy violations by evaluating the potential sanctions for violating policies (Bulgurcu et al., 2010; Siponen & Vance, 2010).

In terms of influencing individual employee behavior, there are two primary vectors routinely utilized to influence employee behavior in the workplace. The first is training, often called “Security Education Training & Awareness” or SETA programs. Another vector frequently utilized to influence cybersecurity behavior in the workplace is composed of various organizational communications designed to influence employee behavior (e.g. “fear appeals” (Johnston & Warkentin, 2010)).

We suggest that cybersecurity training protocols should be contingent on individual differences, rather than a “one size fits all” approach. In the present study, we seek to identify the individual differences that are germane and then identify their relationship with policy compliance intentions. One individual difference of importance is personality type, which is relatively stable over each person’s lifetime. 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 compliance intention motivations, we can create guidelines for authoring various training protocols that are customized to meet the unique needs of diverse cybersecurity users within the workplace, and which will be more effective at influencing the behavior of the trainees.

Although research on cybersecurity policy compliance has expanded in the last few years, there are still gaps in the literature. For instance, the literature that identifies linkages between individual differences and compliance intention has not been integrated into a single model, nor have the various dimensions of individuals been thoroughly explored. In addition, according to Puhakainen et al. (2010), few security compliance studies empirically explore the role of training and compliance. Bulgurcu et al. (2010) highlight the need for additional empirical research on information security awareness education and training. Puhakainen et al. (2010) state “when the aim is to motivate cognitive – and avoid superficial – processing of information, IS security policy compliance training should use learning tasks that are personally relevant to the learners.” This study is designed to identify which individual characteristics have a significant impact on cybersecurity behaviors in order to develop such personally-relevant cybersecurity learning tasks.

Appropriate cybersecurity education programs, especially within the workplace, should be based on an informed deep understanding of the relationships between individual employee psychological profiles and training protocols. Our research is designed to provide such knowledge. In this study, we will develop and empirically validate a comprehensive, yet parsimonious, model of cybersecurity compliance intentions which will be used to construct tailored cybersecurity training protocols. Identifying the factors that motivate compliance among diverse sectors within the workplace has implications for employee selection, assignment (e.g., to specific departments and project teams), and training. Ultimately, this research is designed to identify individual differences (in threat perceptions, sanctions, and other factors), develop psychological profiles which can be used to categorize all employees (including those who may pose an insider threat), construct training protocols that can be used to improve workforce cybersecurity practices, and establish a foundation for the development of customized cybersecurity training modules. Future research includes the adaptation of these protocols into training modules that can be implemented and tested for efficacy.

BACKGROUND LITERATURE

What has the extant research taught us about insider abuse? Recent research, found largely within the Management Information Systems (MIS) research community and supported by theories found in social psychology, criminology, and
other related disciplines, has identified a number of factors that influence individuals to either comply with or violate policies regarding cybersecurity. Extant literature has identified various organizational tools used to combat insider abuse, such as deterrence, prevention, detection, and remediation (Straub and Welke, 1998), managerial communications (Johnston and Warkentin, 2010), and other techniques which can be used to motivate compliance with cyber security practices. On the other hand, perceived feelings of organizational injustice are likely to provoke individual employees to commit acts of internal computer abuse (Willison & Warkentin, 2010), and techniques of neutralization (Siponen and Vance, 2010) are used by employees to rationalize their volitional noncompliant behaviors. Some individual-level factors, especially attitudes and intentions, can be influenced by organizational actions, such as sanctions, rewards, or Security Education, Training, and Awareness (SETA) campaigns (Hollinger and Clark 1982; Puhakainen & Siponen, 2010). Other individual differences are relatively static and cannot be easily influenced, such as morality, gender, and ethnicity. Sanctions (both formal and informal) are found to have an impact in certain circumstances, but only when employees evaluate potential behaviors from a rational choice (cost-benefit) point of view.

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-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 compliance intention motivations, we can establish the guidelines for authoring various training protocols customized to meet the unique needs of diverse cybersecurity users within the workplace.

One of the common personality assessments 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 measured in this test are listed in Table 1. Initial investigations have established linkages between the Big Five personality traits and cybersecurity compliance behaviors (Shropshire et al., 2006). For instance, preliminary investigations have established that the traits of conscientiousness and agreeableness may be strongly linked with an individual employee’s intention to comply with cybersecurity policies and to adopt protective technologies (Major et al., 2006; Shropshire et al., 2006). However, other Big Five traits such as openness, along with individual differences such as the rationality of individual decision making; the degree of alignment with the organization’s goals; cultural factors; or how much an individual may react to emotional appeals (e.g., fear appeals), sanctions, or rewards may also prove to be instrumental in establishing a profile that is associated with the motivation to comply with cybersecurity policies.

<table>
<thead>
<tr>
<th>Big Five Trait</th>
<th>Trait Description (Zhang 2006)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neuroticism</td>
<td>“People [scoring] high on the [neuroticism] scale tend to experience such negative feelings as emotional instability, embarrassment, guilt, pessimism, and low self-esteem”</td>
</tr>
<tr>
<td>Extraversion</td>
<td>“People scoring high on the extraversion scale tend to be sociable and assertive, and they prefer to work with other people.”</td>
</tr>
<tr>
<td>Openness to experience</td>
<td>“[People scoring high on the openness scale are] characterized by such attributes as open-mindedness, active imagination, preference for variety, and independence of judgment.”</td>
</tr>
<tr>
<td>Agreeableness</td>
<td>“People [scoring] high on the agreeableness scale tend to be tolerant, trusting, accepting, and they value and respect other people’s beliefs and conventions.”</td>
</tr>
<tr>
<td>Conscientiousness</td>
<td>“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.”</td>
</tr>
</tbody>
</table>

Table 1: Big Five Personality Trait Descriptions

We seek to understand the role of individual differences, such as the “Big Five” personality traits, on cybersecurity compliance (John & Srivaastava, 1999). One such individual difference is the degree to which each individual is influenced...
by sanctions (Boss et al. 2009; D’Arcy et al 2008; Herath and Rao 2009). Deterrence theory (Akers, 1990; Ehrlich, 1996) 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. But 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, avoiding proper patch management, 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). So SETA programs can inform employees about sanctions, but individuals will cognitively process that information in unique ways. Another important individual difference addresses one’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).

RESEARCH MODEL

Why do some employees comply with organizational cybersecurity policies and others do not? Can these antecedents be influenced with training, sanctions, or other interventions? What can be learned about differences in the way that individuals react to sanctions? Are there certain individual differences, such personality characteristics, which may enable organizations to identify the appropriate job candidates to hire in order to match the goals of the organization? These are the primary questions we wish to address in our study. The model shown in Figure 1 contains the elements which we intend to explore during this study. Preliminary results are presented here, and later findings of our full study will be presented at the conference.

![Figure 1: The Relative Impact of Protection Motivation, Sanctions, and Personality Traits on Cybersecurity Violation Intention](image-url)
METHOD

We apply a factorial survey approach 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 201 usable observations from an online sample of 86 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), each participant was asked to read and respond to an online survey that contained four randomly generated hypothetical scenarios, yielding 344 observations at the vignette level, of which 143 were removed due to failures in the manipulation checks and the content validity (realism) measure. This resulted in 201 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.

After reading a scenario in which Joe ignores a password encryption procedure and engages in a form of information theft, respondents were asked to estimate the chance that they would mirror the employee’s actions under similar conditions. The response options ranged from one to five, with five serving as a “strongly agree” with conducting actions similar to those of Joe. Manipulated as part of each scenario is Joe’s perception of perceived threat severity, perceived threat susceptibility, perceived self-efficacy, perceived response efficacy, perceived response cost, perceived sanction severity, and perceived sanction certainty. The dependent variable in this study is the respondent’s self-reported intention to perpetrate an act of computer abuse (password theft) as described in each scenario. We assessed the Big Five personality traits using a 44-item 5-point Likert scale (John et al. 2008), capturing the distinct factors of agreeableness, conscientiousness, extraversion, neuroticism, and openness.

DATA ANALYSIS AND RESULTS

Model estimation followed an approach similar to Lyons (2008) and Paternoster and Simpson (1996) in which a “random effects” model is used to account for unobserved heterogeneity across respondents, a concern of the factorial survey research design. For the dependent variable, intention to perpetrate computer abuse, the estimated model includes each of the dimensions described by PMT as well as the perceived sanction dimensions of perceived sanction severity and perceived sanction certainty position as direct antecedents of behavioral intent. Subsequent models are provided that test for cross-level interactions involving the Big 5 personality traits.

Results

While the scenarios presented to the participants in the study are in terms of a fictitious character involved in data theft scenario, the factorial survey design allows us to draw inferences to respondent behavior if placed in similar situations. As indicated in Table 2, the results of this study suggest that highly severe consequences for unauthorized data access are significantly more effective in preventing data theft than less severe consequences. Similarly, data protection is more likely to occur in situations in which the protective act does not take much time to complete (low perceived response cost). In terms of sanctioning, the results indicate that highly severe sanctions are more effective in eliciting protective behavior than less severe or certain punishment, while the certainty of the sanctions is non-significant in the determination of protective behavior.
An examination of the Big 5 personality factors as moderating factors on the relationships forming behavioral intent suggests several significant interactions, depicted in Table 3. The results of this cross-level interaction analysis suggest that agreeableness interacts with self-efficacy, such that in their determination of whether to protect sensitive data, more agreeable respondents will place more importance on their ability to protect data than less agreeable respondents. Similarly, compared to their less conscientious peers, more conscientious respondents will find the severity and certainty of possible sanctions stemming from data theft to be more impactful in the decisions of whether or not to protect sensitive data. Finally, in terms of response costs, highly neurotic and open respondents will look more carefully at the costs associated with performing protective acts than their less neurotic or open peers.

Table 2: Random Intercept Model: Behavioral Intention to Commit Computer Abuse

<table>
<thead>
<tr>
<th>Dimension and Level</th>
<th>β</th>
<th>S.E.</th>
<th>T-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Threat Severity *</td>
<td>0.108</td>
<td>0.027</td>
<td>3.926***</td>
</tr>
<tr>
<td>Perceived Threat Susceptibility b</td>
<td>0.062</td>
<td>0.031</td>
<td>1.991</td>
</tr>
<tr>
<td>Perceived Self-Efficacy c</td>
<td>0.002</td>
<td>0.025</td>
<td>0.076</td>
</tr>
<tr>
<td>Perceived Response Efficacy d</td>
<td>-0.040</td>
<td>0.025</td>
<td>-1.577</td>
</tr>
<tr>
<td>Perceived Response Cost</td>
<td>0.227</td>
<td>0.066</td>
<td>3.458**</td>
</tr>
<tr>
<td>Perceived Sanction Severity e</td>
<td>0.061</td>
<td>0.029</td>
<td>2.140*</td>
</tr>
<tr>
<td>Perceived Sanction Certainty f</td>
<td>0.036</td>
<td>0.022</td>
<td>1.664</td>
</tr>
<tr>
<td>Intercept</td>
<td>1.014</td>
<td>0.177</td>
<td>5.725***</td>
</tr>
</tbody>
</table>

Observations (Vignette Level) N = 201

Fit Statistic

AIC = -529.146
BIC = -261.578

Reference levels: high threat severity *; high threat susceptibility b; high self-efficacy c; high response efficacy d; high sanction severity e; high sanction certainty f

* p < 0.05; ** p < 0.01; *** p < 0.001
**Table 3: Cross-level Interactions for Behavioral Intention to Commit Computer Abuse**

<table>
<thead>
<tr>
<th>Respondent Level</th>
<th>$\beta$</th>
<th>T-Value</th>
<th>Scenario Level</th>
<th>$\beta$</th>
<th>T-Value</th>
<th>Interaction $\beta$</th>
<th>T-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreeableness</td>
<td>-0.282</td>
<td>-3.01**</td>
<td>Self-Efficacy</td>
<td>-1.132</td>
<td>-2.23**</td>
<td>0.274</td>
<td>2.18**</td>
</tr>
<tr>
<td>Conscientiousness</td>
<td>-0.298</td>
<td>-2.91**</td>
<td>Sanction Severity</td>
<td>-1.249</td>
<td>-2.15**</td>
<td>0.293</td>
<td>2.14**</td>
</tr>
<tr>
<td>Conscientiousness</td>
<td>-0.265</td>
<td>-2.56**</td>
<td>Sanction Certainty</td>
<td>-0.939</td>
<td>-1.62</td>
<td>0.232</td>
<td>1.68*</td>
</tr>
<tr>
<td>Neuroticism</td>
<td>-0.292</td>
<td>-1.81*</td>
<td>Response Cost</td>
<td>0.359</td>
<td>2.39**</td>
<td>0.129</td>
<td>2.15**</td>
</tr>
<tr>
<td>Openness</td>
<td>-0.478</td>
<td>-2.21**</td>
<td>Response Cost</td>
<td>0.047</td>
<td>0.171</td>
<td>0.171</td>
<td>2.32**</td>
</tr>
</tbody>
</table>

* $p < 0.1$; ** $p < 0.05$

**DISCUSSION**

These initial results confirm that individuals react differently to the same conditions, and imply that the approach we adopt to cybersecurity training must also differentiate between individual employee archetypes. But what are these categories, and how can we differentiate between the employees so we can deliver SETA training that is appropriate for each type? The ultimate goal of this study is to assist in the development and evaluation of a comprehensive framework for enhancing cybersecurity practices in the business sector. In particular, we plan to highlight the cybersecurity perceptions and intentions of diverse personality types. By creating a limited set of unique cybersecurity personality profiles, we will be able to develop customized training protocols that meet the unique needs of each technology user (see Figure 2).

![Figure 2: Depiction of research framework and implications](image-url)

**CONCLUSION**

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 individual react to various influences such as sanctions and organizational communications, such as fear appeals. Therefore, the purpose of this study is to collect data from computer users related to how they perceive cybersecurity threats both inside and outside of 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 develop practices that will help secure businesses against internal security threats.

REFERENCES


