December 2006

Personality and IT security: An application of the five-factor model

Jordan Shropshire
Mississippi State University

Merrill Warkentin
Mississippi State University

Allen Johnston
University of Louisiana Monroe

Mark Schmidt
St. Cloud State University

Personality and IT security: An application of the five-factor model

Jordan Shropshire
Dept of Management & Information Systems
College of Business & Industry
Mississippi State University
P.O. Box 9581
Mississippi State, MS 39762-9581
JDS372@msstate.edu

Merrill Warkentin
Dept of Management & Information Systems
College of Business & Industry
Mississippi State University
P.O. Box 9581
Mississippi State, MS 39762-9581
mwarkentin@acm.org

Allen C. Johnston
College of Business Administration
Department of Computer Information Systems
University of Louisiana Monroe 700 University
Avenue Monroe, LA 71209-0120
318-342-1142 office
318-342-1149 fax
ajohnston@ulm.edu

Mark B. Schmidt
Dept of Business Computer Information Systems
G. R. Herberger College of Business
St. Cloud State University
720 4th Ave. South
St. Cloud, MN 56301
mbschmidt@stcloudstate.edu

ABSTRACT

Despite numerous advances in IT security, many computer users are still vulnerable to security-related risks because they do not comply with organizational policies and procedures. In a network setting, individual risk can extend to all networked users. Endpoint security refers to the set of organizational policies, procedures, and practices directed at securing the endpoint of the network connections – the individual end user. As such, the challenges facing IT managers in providing effective endpoint security are unique in that they often rely heavily on end user participation. But vulnerability can be minimized through modification of desktop security programs and increased vigilance on the part of the system administrator or CSO. The cost-prohibitive nature of these measures generally dictates targeting high-risk users on an individual basis. It is therefore important to differentiate between individuals who are most likely to pose a security risk and those who will likely follow most organizational policies and procedures.

Keywords

Personality, security, five-factor model, technology adoption.

INTRODUCTION

IT security systems are rapidly becoming highly advanced and user-friendly; in fact, some security programs are almost fully automated. However, these systems will only work if they are used properly. Often, the weakest link is the individual user, the employee who neglects to update security patches, change passwords, or run virus scans. They weaken not only their computer's security, but that of the entire network as well. It is these employees who need fully-automated virus detection and anti-spyware programs, automated backups, limited download capability, perimeter controls, and additional support from systems administrators. However, enacting these precautionary measures for all users may not be feasible. Unfortunately, it is difficult to separate prudent employees from those who are likely to pose a serious security risk.

It is the purpose of this research to develop a basis for differentiating among those who are more likely to adhere to IT security guidelines, and those who are not. The factors *agreeableness* and *conscientiousness*, from the five-factor model of personality, are proposed as a means for performing this task. Based on previous research, it is hypothesized that individuals

measuring high in agreeableness and conscientiousness will exhibit IT security-compliant behaviors, and conversely, those with lower measures will be less likely to exhibit IT security-compliant behavior (Cellar *et al.*, 2001).

The following section introduces endpoint IT security. The next section includes a discussion of the shortcomings of technology acceptance theory as a means of approaching the current research problem. The case for adopting personality theory over technology acceptance is then made, and two factors from the five-factor model are then explored as candidates for distinguishing among users who are more likely to exhibit IT security-compliant behavior, and those who are not. Hypotheses regarding the personality factors are made, and a possible research methodology is described. Final conclusions and limitations are then addressed.

BACKGROUND

Endpoint Security

Numerous sources consistently suggest that the greatest threat to most organizations is not the external threat beyond the perimeter (hackers, malware, etc.), but rather the careless or malicious actions of individuals within the organization. Each employee represents an endpoint of the organization's network, and without security-compliant behavior on the part of each and every employee (and other internal constituents), there can be no organizational security. Secure behaviors include making regular backups, changing passwords, scanning for viruses, and many other activities identified by Whitman (2003) and others. Employees often lack awareness of the organization's security policies and procedures (Adams and Sasse, 1999; Furnell, et al, 2002; Siponen, 2001) and are, therefore, not equipped to be in compliance. They also lack the technical expertise to recognize sources of security threats (downloading files, web surfing behavior, etc.). It is incumbent on IT management, therefore, to understand the endpoint security problem in the organization, and to address the sources of threat in an appropriate manner.

Technology Acceptance

Because of the unique nature of information technology security, opportunities to apply previous IS research are limited. The research paradigm collectively known as *technology acceptance* has long sought to explain the factors which determine initial adoption and continued use of technology by individuals (Venkatesh *et al.*, 2003). However, technology acceptance theory may not be applicable for three reasons:

(1) two of the most powerful constructs used to explain technology acceptance are *perceived usefulness* and *perceived ease of use*, which are defined as the degree to which an individual expects to see performance enhancements, and the degree to which an individual believes that using a particular system should be free of effort, respectively (Davis, 1989). IS security often involves additional effort, which individuals may also interpret as impeding their computing performance, even as they continue to use the security mechanism (Warkentin *et al.*, 2004). In these instances, perceived usefulness and ease of use will have little explanatory power.

(2) The primary focus of technology acceptance research is on the individual's attitudes regarding a specific technology (Bhattacherjee, 2001). To assess whether an individual will adopt a given technology, researchers must instantiate a technology acceptance metric to fit that particular technology (Venkatesh *et al.*, 2003). Due to the rapidly evolving nature of IS security and the broad range of artifacts which fit into the IS security category, it may be infeasible to develop a traditional technology acceptance metric for every scenario.

(3) In most models of technology acceptance, behavioral intention is based partially on the individual's attitudes towards a given technology (Davis, 1989; Taylor and Todd, 1995; Venkatesh *et al.*, 2003). Because an individual cannot have an attitude towards a technology which has not yet been conceived, it would be impossible to project an individual's reaction to future technologies using the technology acceptance approach.

Although technology acceptance has contributed many advances toward understanding the relationship between individual attitudes and technology acceptance, it has limitations which should be reconciled prior to its utilization in IS security.

Personality versus Attitude

Instead of focusing on the individual's attitude towards a given technology, this research concentrates on various dimensions of the individual's personality and his relationship with information technology security. There are two beneficial properties associated with this approach:

(1) **Stability**. Personality characteristics are stable over time (Buss, 1988; Brody, 1988; Funder, 1991), and could be used toward making relatively longer-term projections than is possible with attitudes (Digman, 1990; Fishbein and Ajzen, 1975).

(2) **Presence**. Whereas an individual cannot have an attitude towards a technology which he or she is unaware of, he or she will always have a measurable personality (Goldberg, 1993; Wiggins, 2003). Therefore, it might be possible to project an individual's propensity to maintain current IS security standards, as well as those which have not yet been conceived, based on characteristics of his or her personality that may play a role in shaping his or her attitudes.

Personality traits have long been used to interpret and predict various factors in diverse environments (Funder, 1991; James and Mazerolle, 2002; John and Robbins, 1993). For example, in a study of organizational innovation, it was found that employees whose personalities are low in risk, and high in achievement and innovativeness, are most likely to become champions of innovation (Howell and Higgins, 1990). Personality has also been applied to human resources management, including issues such as psychological contracts (Raja *et al.*, 2004), relationship stability (Attridge *et al.*, 1995), and participation in self-managed work groups (Thoms *et al.*, 1996). Within the realm of information systems research, progress is being made towards correlating personality characteristics with the critical aptitudes that individuals must possess for successful careers in various information technology fields (Pemberton *et al.*, 2005), and utilizing personality metrics for IS project team selection (Klein *et al.*, 2002).

Because of their widespread appeal and range of applications, there are multiple conceptualizations of the basic personality dimensions. The implication of this phenomenon is lack of a clear standard (Goldberg, 1971). However, the five-factor model of personality stands apart as a leading theoretical model, and has enjoyed increasing popularity over the past twenty years (Geller and Wiegand, 2004).

Five-factor Model

The development of the five-factor model began with the work of Allport and Odbert (1936), in which some eighteen thousand personality-related terms were identified. By 1945 the list had been reduced to thirty-five variables (Cattell, 1945). These variables were eventually conceptualized into five strong factors (Tupes and Christal, 1961). After repeated validations, they eventually became known as the *big five* (Goldberg, 1981). Since the inception of the *big five*, a multitude of similar five-factor models have been proposed, including models such as those prescribed by Botwin and Buss (1989), Costa and McCrae (1985), Goldberg (1981), and Conley (1985). However, one of the most commonly cited models is the *big five trait taxonomy*, suggested by Oliver P. John and S. Srivastava (1999). This taxonomy, shown in Table 1, includes the factors *extraversion*, *agreeableness*, *conscientiousness*, *neuroticism*, and *openness*. It is being proposed here as a means of identifying individuals who are most likely to demonstrate IT security-compliant behavior. There are two salient advantages to choosing the five-factor model over other specific factors.

Factor Name	Factor Description
Extraversion Energy Enthusiasm	"An energetic approach to the social and material world and includes traits such as sociability, activity, assertiveness, and positive emotionality."
Agreeableness Altruism Affection	"Contrasts a prosocial and communal orientation towards others with antagonism and includes traits such as altruism, tender-mindedness, trust and modesty."
Conscientiousness Control Constraint	"Socially prescribed impulse control that facilitates task and goal oriented behavior, such as thinking before acting, delaying gratification, following norms and rules, and planning, organizing, and prioritizing tasks."
Neuroticism Negative-Affectivity Nervousness	"Contrasts emotional stability and even-temperedness with negative emotionality, such as feeling anxious, nervous, sad, and tense."
Openness Originality Open-mindedness	"In contrast to closed-mindedness, describes the breadth, depth, originality, and complexity of an individual's mental and experiential life."

Table 1: Five-factors as described by John and Srivastava (1999)

One of the primary advantages of the five-factor model is the generalizability inherent in its systematic and comprehensive approach to personality (Arthur and Graziano, 1996; Goldberg, 1993). The factors are not meant to represent a specific theoretical perspective, but rather a complete taxonomy of terms which allow individuals to describe themselves and others (John and Srivastava, 1999). This generalizability permits use of the model across many research disciplines, including those which may be similar in nature to IT security.

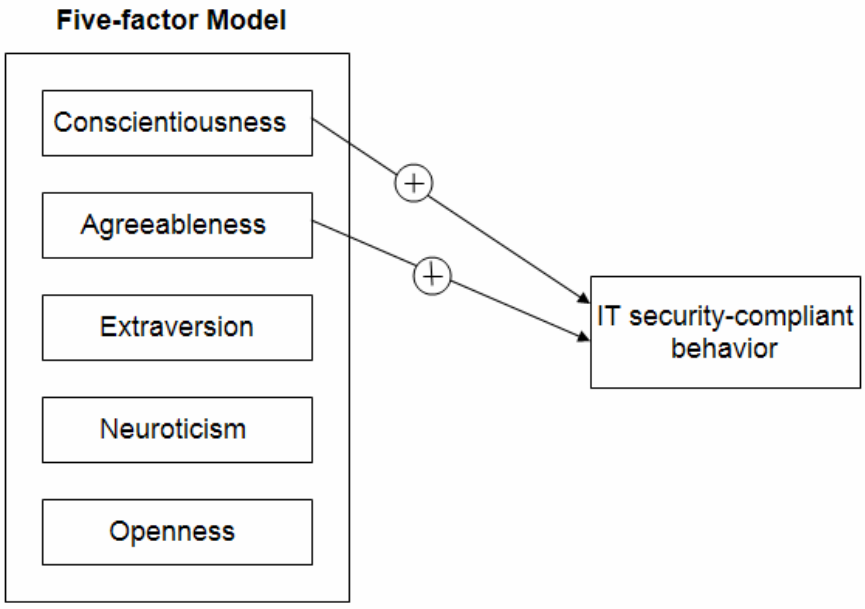

Figure 1: Relationship between five-factor model and IT security-compliance

A second advantage of using the five-factor model is that the behavioral patterns associated with the factors are well known in comparison to the large number of specific factors (Cellar *et al.*, 2001). Numerous organizational studies have identified a significant inverse relationship between accident involvement and the personality factor conscientiousness (Arthur and Graziano, 1996; Cellar *et al.*, 2001). Individuals who rated themselves as higher in delaying gratification, thinking before acting, following norms and rules, and planning and organizing tasks were less likely to be involved in accidents than those who rated themselves as lower on the same attributes (Arthur and Graziano, 1996). Based on the findings from these studies, the first hypothesis is presented (see Figure 1):

H_1: Conscientiousness is positively related to IT security-compliant behavior.

In addition, organizational safety and agreeableness have also been found to have a significant positive relationship; those who rated themselves as having a stronger interpersonal orientation were also less likely to be involved in accidents (Cellar *et al.*, 2001). Given the demonstrated relationship between agreeableness and safety, the second hypothesis is stated:

H_2: Agreeableness is positively related to IT security-compliant behavior.

PROPOSED METHODOLOGY

In order to evaluate the nature of the relationship between the five personality factors and IT security-compliant behavior, the hypotheses will be tested using a subset of Goldberg's Unipolar Markers and observations of IT security-related behavior. For this research, the sample is approximately one hundred and twenty staff, faculty, and graduate assistants employed by the college of business at a medium sized research institution in the US. This sample represents a diverse set of experienced computer users who are the endpoints of a single network environment with a consistent set of environmental factors.

Goldberg's Unipolar Markers is a one-hundred item personality assessment developed to measure the five personality factors (1992). A subset of forty measures is adopted, twenty of which operationalize agreeableness and a second twenty of which are measures for conscientiousness. In line with previous studies, a participant's score for each factor is the sum of his or her ratings on the twenty items which compose a factor after the appropriate items have been reverse-coded (Arthur and Graziano, 1996).

The dependent variable, IT security-compliant behavior, is a composite measure of actions users must perform in order to comply with IT security. Currently, the authors are developing the variable independently of this research. The behaviors included in the variable were derived from a list of the top IT security procedures identified by IT managers and directors (Whitman, 2003), augmented by other procedures suggested by experts in computer security. Some of the security

procedures include use of passwords, media backup, virus protection software, and employee education. A panel consisting of four IT security practitioners and four IT security academians is currently performing a content validity assessment of the newly-selected construct dimensions.

In a manner similar to Cellar *et al.* (2001), the data analysis will consist mainly of regression analysis. Each of the five personality factors will be tested using stepwise regression analysis to determine the extent to which it can be used to predict IT security violations.

LIMITATIONS

A salient limitation in this paper is the sole focus on personality as a determinant of security-related behavior. Other behavioral elements may play a critical role in behavior – these factors have not been treated in the current study. In addition, sociological forces may shape the individual's perceptions of organizational abuse and discipline, and thus his or her actions (Straub and Nance, 1990; Straub and Welke, 1998). These forces may include social bonds with other organizational members, or even social learning (Lee and Lee, 2002).

CONCLUSION

The purpose of this research is to propose a method for identifying individuals who are most likely to commit IT security infractions based on various dimensions of their personality. The research model is based on a version of the five factor model described by John and Srivastava (1999). It was hypothesized that conscientiousness and agreeableness have a significant relationship with IT security-compliant behavior. A method for testing the hypotheses was also described. Items from Goldberg's Unipolar Markers were used to measure agreeableness and conscientiousness. A composite variable, IT security-compliant behavior, was suggested as a means for measuring user behavior. If further testing reveals that personality measures are a reliable indicator IT security compliance, then it may be possible to use these measures to minimize security risks within the organization.

REFERENCES

1. Adams, A. and M.A. Sasse (1999). "Users are not the enemy." Communications of the ACM **42**(12), December: 40-46.
2. Allport, G. and H. S. Odbert (1936). "Trait-names: A psycho-lexical study." Psychological Monographs **47**(211).
3. Arthur, W. and W. Grazziano (1996). "The five-factor model, conscientiousness, and driving accident involvement." Journal of Personality **64**(3): 594-618.
4. Attridge, M., E. Berscheid and J. A. Simpson (1995). "Predicting relationship stability from both partners versus one." Journal of Personality & Social Psychology **69**(2): 254-268.
5. Bhattacherjee, A. (2001). "Understanding information systems continuance: An expectation-confirmation model." MIS Quarterly **25**(3): 351-370.
6. Botwin, M. D. and D. M. Buss (1989). "Structure of act-report data: Is the five-factor model of personality recaptured?" Journal of Personality and Social Psychology **56**: 988-1001.
7. Brody, N. (1988). Personality: In Search of Individuality. New York, NY, Academic Press.
8. Buss, A. H. (1988). Personality: Evolutionary Heritage and Human Distinctiveness. Hillsdale, NJ, Lawrence Erlbaum Associates, Inc.
9. Cattell, R. B. (1945). "The principal trait clusters for describing personality." Psychological Bulletin **42**: 129-161.
10. Cellar, D. F., Z. C. Nelson and C. M. Yoke (2001). "The five factor model: Investigating the relationships between personality and accident involvement." Journal of Prevention & Intervention in the Community **22**(1): 43-52.
11. Conley, J. J. (1985). "Longitudinal stability of personality traits: A multitrait-multimethod-multioccasion analysis." Journal of Personality and Social Psychology **49**: 1266-1282.
12. Costa, P. T. and R. R. McCrae (1985). NEO Personality Inventory Manual. Odessa, FL, Psychological Assessment Resources.
13. Costa, P. T. and R. R. McCrae (1992). NEO PI-R Professional Manual. Odessa, Fl, Psychological Assessment Resources.

14. Davis, F. D. (1989). "Perceived usefulness, perceived ease of use, and user acceptance of information technology." MIS Quarterly **13**(3): 319-339.
15. Digman, J. M. (1990). "Personality structure: Emergence of the five-factor model." Annual Review of Psychological Psychology **41**: 417-440.
16. Fishbein, M. and I. Ajzen (1975). Belief, Attitude, Intention and Behavior: an Introduction to Theory and Research. Reading, MA, Addison-Wesley.
17. Funder, D. C. (1991). "Global traits: A neo-Allportian approach to personality." Psychological Science **2**: 31-39.
18. Furnell, S.M., Gennatou, M. and Dowland, P.S. (2002). "A prototype tool for information security awareness and training." Logistics Information Management **15**(5/6): 352 - 357.
19. Geller, E. S. and D. M. Wiegand (2005). "People-based safety: Exploring the role of personality in injury prevention." Professional Safety (December): 28-36.
20. Goldberg, L. R. (1971). "A historical survey of personality scales and inventories." Advances in Psychological Assessment **2**: 293-336.
21. Goldberg, L. R. (1981). Language and individual differences: The search for universals in personality lexicons. Review of Personality and Social Psychology. L. Wheeler. Beverly Hills, CA, Sage. **2**.
22. Goldberg, L. R. (1992). "The development of markers for the big-five factor structure." Psychological Assessment. **4**(1): 26-41.
23. Goldberg, L. R. (1993). "The structure of phenotypic personality traits." American Psychologist **48**: 26-34.
24. Howell, J. M. and C. A. Higgins (1990). "Champions of organizational change: Identifying, understanding, and supporting champions of technological innovation." Organizational Dynamics **19**: 40-55.
25. James, L. R. and M. D. Mazerolle (2002). Personality in Work Organizations. Thousand Oaks, California, Sage Publications.
26. John, O. P. and R. W. Robbins (1993). Gordon Allport: Father of the five factor model. Fifty Years of Personality Psychology. K. H. Craik, R. Hogan and R. Wolfe. New York, NY, Plenum.
27. John, O. P. and S. Srivastava (1999). The big five trait taxonomy. Handbook of Personality Theory and Research. L. Pervin and O. P. John. New York, The Guilford Press.
28. Kendrick, D. T. and D. C. Funder (1988). "Profiting from controversy: Lessons from the person-situation debate." American Psychologist **43**: 23-34.
29. Klein, G., J. J. Jiang and D. B. Tesch (2002). "Wanted: project teams with a blend of IS professional orientations." Communications of the ACM **45**(6): 81-87.
30. Lee, J. & Lee, Y. (2002) "A Holistic Model of Computer Abuse Within Organizations." Information Management & Computer Security. 10(2): 57-63.
31. Pemberton, A., J. M. Pemberton, J. M. Williamson and J. W. Lounsbury (2005). "RIM professionals: A distinct personality?" Information Management Journal **39**(5): 54-60.
32. Pervin, L. A. (1994). "A critical analysis of current trait theory" Psychological Inquiry **5**(2): 103-113.
33. Raja, U., G. Jones and F. Ntalianis (2004). "The impact of personality on psychological contracts." Academy of Management Journal **47**(3): 350-367.
34. Siponen, M. T. (2001). "Five dimensions of information security awareness," Computers and Society **31**(2): 24-29.
35. Straub, D. & Nance W. (1990). "Discovering and Disciplining Computer Abuse in Organizations: A Field Study." MIS Quarterly. **14**(1): 45-60.
36. Straub, D. & Welke, R. (1998) "Coping with Systems Risk: Security Planning Models for Management Decision Making." MIS Quarterly. **22**(4): 441-469.
37. Taylor, S. and P. Todd (1995). "Understanding information technology usage: A test of competing models." Information Systems Research **6**(4): 167-187.
38. Thoms, P., K. S. Moore and K. S. Scott (1996). "The relationship between self-efficacy for participating in self-managed work groups and the big five personality dimensions." Journal of Organizational Behavior **17**(4): 349-362.

39. Tupes, E. C. and R. C. Christal (1961). Recurrent personality factors based on trait ratings. Lackland Air Force Base, TX, USAF: Aeronautical Systems Division, Personnel Laboratory.

40. Venkatesh, V., M. G. Morris, G. B. Davis and F. D. Davis (2003). "User acceptance of information technology: Toward a unified view." MIS Quarterly **27**(3): 425-478.

41. Warkentin, M., K. Davis and E. Bekkering (2004). "Introducing the check-off password system (COPS): An advancement in user authentication methods and information security." Journal of End User Computing **16**(3): 41-58.

42. Waller, N. G. and Y. S. Ben-Porath (1987). "Is it time for clinical psychology to embrace the five-factor model of personality?" American Psychologist **42**: 887-889.

43. Whitman, M. (2003). "Enemy at the gates: Threats to information security." Communications of the ACM **46**(8): 91-95.

44. Wiggins, J. S. (2003). Paradigms of Personality Assessment. New York, Guilford Press.