Journal of Information Security, **2013, 4, 203-212**
http://dx.doi.org/10.4236/jis.2013.44023 Published Online October 2013 (http://www.scirp.org/journal/jis)

Personality Traits and Cognitive Determinants—An Empirical Investigation of the Use of Smartphone Security Measures

Jörg Uffen, Nico Kaemmerer, Michael H. Breitner
Information Systems Institute, Leibniz Universität, Hannover, Germany
Email: uffen@ccc.uni-hannover.de, nico@kaemmerer-ilten.de, breitner@iwi.uni-hannover.de

Received June 18, 2013; revised July 20, 2013; accepted July 28, 2013

ABSTRACT

In the last years, increasing smartphones' capabilities have caused a paradigm shift in the way of users' view and using mobile devices. Although researchers have started to focus on behavioral models to explain and predict human behavior, there is limited empirical research about the influence of smartphone users' individual differences on the usage of security measures. The aim of this study is to examine the influence of individual differences on cognitive determinants of behavioral intention to use security measures. Individual differences are measured by the Five-Factor Model; cognitive determinants of behavioral intention are adapted from the validated behavioral models theory of planned behavior and technology acceptance model. An explorative, quantitative survey of 435 smartphone users is served as data basis. The results suggest that multiple facets of smartphone user's personalities significantly affect the cognitive determinants, which indicate the behavioral intention to use security measures. From these findings, practical and theoretical implications for companies, organizations, and researchers are derived and discussed.

Keywords: Security Measures; Personality Traits; Behavioral Models; Mobile Security; Smartphones

1. Introduction

In the last years, mobile devices have introduced a new dimension into life and work. Increasing capabilities have caused a paradigm shift in the way users view and use mobile devices [1]. Smartphones and other mobile devices, such as tablet PCs, are small, easy to carry and powerful in computational and storage capabilities. Particularly smartphones and tablet PCs are being used in a business context and replacing classic business mobile phones and to some extent, notebook PCs. Organizational decision-makers have increasingly come to accept the use of mobile and private devices and applications in the organizational IS environment [2]. Hence, research studies emphasize management's concerns about the protection of organizational information asset [1,3]. Smartphone users' behavior in different situations and how they cope with security measures become important in the organizational information security context. While researchers focus on technical issues or on organizational perspectives of mobile security (e.g. [1]), behavioral research is very limited up to now [3].

The attempt of this study is to examine how behavioral cognitive determinants affect the behavioral intention to use smartphone security measures. In information security research, the adoption of behavioral models, such as theory of planned behavior (TPB) and core constructs of the technology acceptance model (TAM), is well established to explain and predict user behavior (for a list see, for example [4,5]. Only a few studies have investigated the rooting behavioral determinants that lead to different attitudes and behavioral intentions. Fishbein and Ajzen [6] recognized the potential importance of additional external behavioral influence factors that are outside the TPB. The authors explicitly stated that individual differences in personality are external variables that influence a specific behavior indirectly through mediating cognitive constructs contained within the TPB [6,7]. Therefore, this study investigates the relationship between personality traits and cognitive behavioral models. Other research studies, for example Devaraj *et al*. [8] and Nov and Ye [9], investigated the relationship between personality traits and TAM in a different IS context. The authors found that personality traits are useful predictors of attitudes and beliefs. Wang [2] incorporated personality traits into the IS continuance model to examine the in-

fluence of personality traits on an individual's IS continuance intention. The author suggested that personality traits and cognitive determinants on behavior, as provided by the TPB and the TAM constructs of attitude and behavioral intention, might be integrated into a single model. We make a theoretical contribution by conceptualizing that smartphone users' actions and decisions are significantly driven by their personalities. Personality is measured using the five-factor model (FFM) [10]. We explore the following research question by testing an integrated personality model:

How do smartphone users' personality traits influence the cognitive determinants of their usage of security measures?

This paper is structured as follows: first, we provide a theoretical basis and outline the identified research gap. After presenting the model development and analysis, we report and discuss the results of our empirical investigation. Finally, we conclude with a discussion of implications for practice and research, limitations, and an outlook for future research.

2. Theoretical Background

2.1. Key Areas Comprising Mobile Security

Rapid changes in the use of mobile devices have caused a paradigm shift in the information security context. The definition of mobile devices includes portable electronic devices that store potentially critical information and data [11]. Although this broad definition includes laptops and notebooks or personal digital assistants (PDA), the focus of this paper lies on multi-function pocket and handheld devices such as smartphones or tablet PCs (in the following, referred to as smartphones) that use touch-sensitive screens. Due to increasing mobility, easier communication, and processing ability, individuals carry smartphones with critical information and data with them [12], which results in an even larger user base [13]. Besides the ability to run many applications, individuals can access, store, and manipulate private data, as well as critical information from organizational networks such as emails, contact details of clients and suppliers, and calendar items [11,12]. To prevent data loss, smartphones typically include security measures, also referred to as countermeasures or security mechanisms [4,14], such as password protection, backup and restore, and remote device wipe [12]. Organizations integrate security aspects of employee-owned and organizational mobile devices into their information security strategies and policies. Therefore, national and international organizations issued fundamental best-practices, guidelines and standards, such as the International Standards Organization's (ISO) Code of Practice (ISO/IEC 27001; ISO/IEC 27002) or National Institute of Standards and Technology (NIST) special publications such as SP 800 - 124, which provide recommendations regarding the implementation and management of security measures for smartphones. But these standards or guidelines are generic in scope and do not focus on the different security requirements within organizations.

Even if challenges for securing smartphones are very similar to those encountered with personal computers or laptops and notebooks, often smartphone users themselves are the private owner and and in some cases responsible for the device's configuration and use of security measures [11]. For example, optionally activated security measures bear the risk that users are not willing to actively enable them [12]. For this reason, it is essential to understand the cognitive processes of smartphone users that lead to the actual usage of security measures for smartphones. Currently, only few research studies have started to incorporate cognitive variables into behavioral models that consider the use of different security measures for smartphones [12]. For example, in their research study, Clarke and Furnell [15] elaborated that a significant proportion of smartphone users do not enable PIN-based authentication. The authors examined the attitudes of smartphone users towards PIN- and biometric based security measures. Ben-Asher *et al*. [16] surveyed smartphone users' security needs and concerns, as well as their awareness of security measures. Results suggest that the needs of smartphone users are diverse and increasing awareness encourages users to activate simple security measures. Using protection motivation theory, Tu and Yuan [12] conceptualized a research model that provides an understanding on how smartphone users behave in coping with security threats of loss and theft. These studies and concepts emphasize that smartphone users' cognitive factors are diverse and depend on the influence of other external variables such as individual differences. Prior literature did not reveal an accepted and integrated model that investigates the influence of personality traits on security-related behavior in a smartphone user context.

2.2. Personality Traits and Behavioral Cognition Models in IS Research

The investigation of individual differences has become omnipresent in IS research. Researchers have incorporated related cognitive and personality-related variables into various IS success outcome models in order to predict and explain actual behavior. The integration of personality traits in behavioral cognition models is a relatively young research area in the IS domain. Personality researchers use classification systems that summarize individual differences in personality into fundamental facets of each individual. These traits determine cognitive and behavioral patterns that remain more or less sta-

ble across different situations [17]. Personality traits are commonly referred to as the agile organization within the human being "of those psycho physiological systems that determine his characteristic behavior and thought" ([18], p. 28). The most frequently used taxonomy in personality research is the FFM [19]. The FFM, a parsimonious and comprehensive model of personality, became widely accepted in personality research because its validity was verified by multiple empirical studies [19,20]. Despite criticism of the number and labels of FFM factors (e.g. [19]), a number of beneficial properties are associated with the use of the FFM: stability, presence, and collective appreciation [17]. Its five broad traits are generally characterized as follows (e.g. [10,17,19]):

1) Extraversion is the degree to which an individual is cheerful, assertive, ambitious, and social;

2) Agreeableness is the tendency to be trustful, straightforward, helpful, and willing to cooperate;

3) Persistence, self-control, self-discipline, and dutifulness represent conscientiousness;

4) Openness to experience indicates an appreciation for variety of creativity, flexibility, adventurousness, and imagination; and finally,

5) Anxiety, pessimism, impulsiveness and personal insecurity are related to neuroticism.

To understand the link between a smartphone user's personality and his or her influence factors of actual behavior towards the use of security measures, cognitive processes must be taken into account. As proposed by Devaraj *et al*. [8], the influence of personality traits on behavior is mediated by cognitions, as implied by the TPB or the TAM. TPB and TAM are the most widely applied models of goal-specific cognition and are widely supported by research studies for their predictive power [4,8]. Both models are an adaptation of the theory of reasoned action (TRA), which implies that intentions are proximal cognitive antecedents of actions or behavior. TAM determines that attitudes toward the usefulness and ease of use of an innovative technology are factors in its adoption and use [21]. In TPB, intentions index the motivation to perform a specific action and are determined by three constructs: attitudes (ATT), subjective norm (SN), and perceived behavioral control (PBC). The PBC construct extends TPB from TRA to account for requisite resources necessary for performing a behavior [7]. The SN construct represents an individual's beliefs as to whether a specific behavior is accepted and encouraged by people who are important to her or him [7]. In general, ATT represents an individual's overall evaluation of a specific behavior. Within the context of this research study, ATT constitutes an individual's beliefs that taking security measures is a desirable behavior that helps to enhance the protection of smartphones. Given that TAM is tailored for modeling user acceptance of IS objects, we adapted both attitudinal TAM constructs, perceived usefulness (PU) and perceived ease of use (PEOU), to explain the attitude's impact on behavioral intention. More specifically, in our case, PU determines the degree to which a smartphone user believes that using specific security measures will enhance the protection level of his or her smartphone. The second attitudinal TAM construct, PEOU, denotes the degree to which a smartphone user believes that using security measures for smartphones will be effortless. If a smartphone user perceives the result of a certain behavior as being positive, he or she will form positive attitudes towards the adoption or use of this specific security measure. In comparison to PBC, PEOU represents the individual beliefs about the degree of effort applied, while PBC can be seen as a control belief and situational perception. A smartphone user might perceive that a specific security measure is easy to use, but could feel that she or he does not have control over the adoption or use. As mentioned above, smartphones have different types of security measures in place. Therefore, we decided to determine these behavioral constructs by regarding multiple security measure rather than a single one. Because there is little research in this field yet, we believe that a more global focus on security measures is beneficial for practitioners and researchers alike.

3. Research Model and Hypotheses

Personality research shows that personality traits vary in their respective relevance, but are resistant to transformation [22]. Prior meta-analytic evidence has demonstrated that specific FFM traits are more relevant in explaining different factors of behavior than others [19]. Therefore, specific personality traits are hypothesized to be related to some, but not each and every one of the cognitive constructs. A hypothesized relationship is relevant when it is appropriate, grounded in, and supported by theoretical and empirical research studies.

The aim of this study is to provide a general link between personality traits, cognitive factors, and the respective behavior. Therefore, behavioral intentions are the dependent variable in our integrated model (**Figure 1**).

Assessing intentions rather than actual behavior is theoretically and technically justified. Despite criticism that most critical limitation of TAM or TPB studies is the use of self-reported data (e.g. [23]), several authors have shown a strong and consistent relationship between behavioral intention and actual behavior (e.g. [24]). In our case, the technical measurement of the actual usage of security measures is argued to be difficult due to the sensitive context of information security (e.g. [25] and the large and diverse sample sizes [26]. Despite theoretical agreement that PU, PEOU, SN and PBC predicts behav-

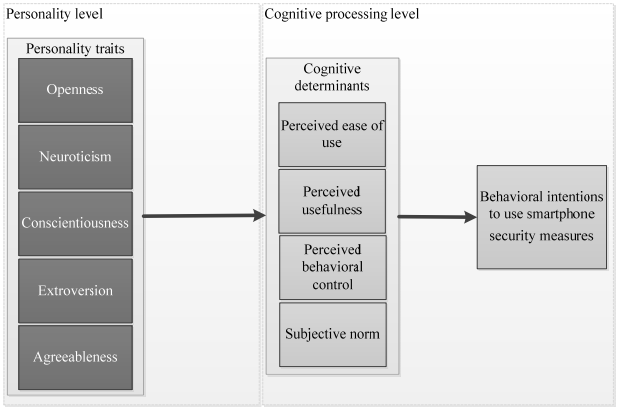

Figure 1. Integrated Research Model.

ioral intentions, prior research has shown a strong and consistent empirical relationship between these constructs (e.g. [4,8]).

Hypothesis (*H*) 1*a*-1*d*: PEOU (H1a), PU (H1b), SN (H1c) and PBC (H1d) are positively associated with the behavioral intention toward the use of security measures

Individuals with an open personality are characterized as being adventurous, creative, intelligent, imaginative, unconventional, and receptive to new and innovative ideas [17]. Associated with various cognitive skills and abilities in individuals, openness is characterized as the motivational tendency to critically examine information, reflection on ideas, and the cognitively differentiated interpretation of information in multiple scenarios [27]. A high degree of openness, with its facets of a deeper scope of awareness and less conscious in tradition [22], promotes that smartphone users deal with potential security risks that might affect their smartphones. This is expected to result in a positive judgment about the utility of security measures in general. These facets and cognitive processes are hypothesized to lead to positive attitudes and values towards the perceived ease of use and usefulness of security measures. Those individuals who are high in openness are less concerned with the change implicit in adopting a new technology [8]. In their meta-analytic review, Judge *et al*. [20] demonstrated that openness is positively related to self-efficacy and the motivation toward the accomplishment of self-set targets. In addition, Barrick *et al*. [19] emphasized that openness is positively related in learning experiences and proficiency. Therefore, more open smartphone users will find it easy to use a security measure and will form positive attitudes towards their own learning experience and capacity to perform.

*H*2*a-c*: Openness is positively associated with attitudes towards the perceived ease of use (H2a), perceived usefulness (H2b), and perceived behavioral control of security measures (H2c)

Neuroticism is characterized by anxiety, pessimism, hostility, and personal insecurity [17]. Individuals who score high in neuroticism tend to avoid situations of taking control and show low motivation toward goal-setting [20]. In addition, prior research demonstrated that one of the facets of neuroticism, anxiety, is negatively related to computer self-efficacy [28]. As a result, neurotic smartphone users tend to feel insecure or nervous that they do not have control over using a security measure. Further, Devaraj *et al*. [8] have shown that emotionally stable individuals, the counterpart of neurotic individuals, are likely to view innovative technical advances as being helpful and important. Due to a lack of confidence and optimism, we expect that if a highly neurotic smartphone user views the use of security measures with skepticism, he or she will form negative attitudes, because it is believed that a potential action cannot make a significant difference in protecting their smartphone.

*H*3*a*, *b*: Neuroticism is negatively associated with the attitude towards perceived usefulness (H3a) and perceived behavioral control of security measures (H3b).

Conscientiousness, a personality trait that is associated with intrinsic motivation to achieve, competence, persistence, and being careful, is one of the most important traits within the research of information security behavior [1,29]. Prior research emphasized a positive relationship between conscientiousness and mindfulness in IT innovations [27], and a positive relation to security concerns [30]. Conscientious smartphone users tend towards purposeful and careful reactions before prematurely employing inefficient security measures. In particular, conscientious smartphone users are more likely to be intrinsically motivated to use security measures to protect their smartphones. This cognitive processing is expected to result in a positive attitude toward the usefulness of the security measure. In addition, individuals with high levels of conscientiousness are more likely to take responsebility [17]. Together with the facet of self-control and due to the tendency of intrinsic motivation to perform, we posit that conscientiousness will interact with PBC in determining behavioral intentions. If a smartphone user forms positive beliefs in his or her capacity to use security measures, conscientiousness will increase those beliefs and result in positive behavioral intentions to use these security measures.

*H*4*a*: Conscientiousness is positively associated with the attitude towards the perceived usefulness of security measures.

*H*4*b*: Conscientiousness moderates the relationship between the attitude perceived behavioral control and behavioral intentions to use security measures.

Individuals who score high in extraversion are characterized as being cheerful, energetic, gregarious, ambitious and optimistic [19]. In addition, they seek out new excitements and opportunities [31] and value interper-

sonal relationships [19]. For example, in training situations, research results indicate that extraverted individuals are more likely to be active and involved in opportunities to provide and obtain information in specific situations [19]. Extraverted individuals tend to perform a specific behavior that is viewed as being desirable by significant others. In this regard, we expect that extraverted smartphone users will form positive intentions to use security measures as long as significant others think that this is acceptable.

*H*5: Extraversion moderates the relationship between subjective norm and behavioral intention to use security measures.

Agreeableness is the trait that implies cooperating, nurturing other individuals, and being helpful and considerate [17]. Prior meta-analytic evidence has demonstrated that agreeableness, like extraversion, is particularly relevant when performance involves interaction with other people [19]. Korukonda [32] demonstrated that agreeableness is negatively related to computer anxiety. Individuals high in agreeableness are sensitive towards other's thoughts and opinions. Therefore, it is hypothesized that agreeable smartphone users will reveal themselves to use security measures when significant others think the same as they do. This leads to the assumption that agreeableness acts as a moderator of the relationship between subjective norm and intention towards the use of security measures.

*H*6: Agreeableness moderates the relationship between subjective norm and behavioral intentions to use security measures.

4. Research Methodology

4.1. Explorative Data Collection Procedure

Kotulic and Clark [33] emphasized that collecting acceptable empirical organizational data in this sensitive context of information security is quite challenging. To gain an acceptable number of observations, we decided to use a student sample. The rationale for using a student sample was to gather acceptable explorative data, given our unique focus on personality traits and behavioral cognition models. The objective of this study is to shed light in the explanation of cognitive processes of smartphone users that lead to specific behavior towards security measures. Personality traits are shown to be relatively stable across situations in an individual's lifespan, especially beyond adulthood [17]. Therefore, a student sample is adaptable into an organizational context. Another reason is that younger individuals, mostly represented through students, have been shown to use mobile devices most frequently [22,34] and are more open to all kinds of innovations and are often the first to adopt them [35]. Although we acknowledge the criticism of the use of student samples due to their limited representativeness or external validity, the appropriateness and usefulness of student samples in the specific context of personality traits and information security has been demonstrated in different research studies (e.g. [22]).

Participants were contacted via university social networks, email, and closed groups in social networks (e.g. Facebook, Xing). Participation was voluntary and no course credits or incentives were given. But participation was motivated by a promise to share the results. The survey was hosted using a secure university-based tool; anonymity and confidentiality were guaranteed. All questionnaires were completed with a web-based survey. A total of 526 undergraduate and graduate business students from a large university participated. Gender was nearly equally balanced with 40% male and 60% female. The largest percentage (65%) of respondents was in the age group of 21 - 29. About 86% of the sample indicated that they use apps, messaging, e-mails, and make calls multiple times a day, indicating that these individuals are experienced smartphone users. In order to ensure a high level of validity, only those questionnaires that were entirely complete were used in the study. The final sample frame contained 435 responses that can be considered sufficient. **Table 1** provides an overview of the demographic statistics.

Table 1. Demographic statistics.

Criteria	Frequency	Percentage
Gender		
Male	174	40
Female	261	60
Range of age		
<21	84	19.3
21 to 29	284	65.3
30 to 39	33	7.6
40 to 49	18	4.1
50 to 59	9	2.1
>59	7	1.6
Level of education		
Student	23	5.3
Secondary modern school	5	1.1
High school diploma	48	11
Higher education entrance qualification	199	45.7
University degree	159	36.6
Not stated	1	0.2

To test for non-response bias, we compared those who responded within a few days with late respondents using t-test comparison of means for measurement items. No significant differences between the early and late respondents could be identified, so non-response bias was not an issue in this study.

4.2. Operationalization of Measurement Items and Instrumentation

The items for constructs were adapted with the help of validated items from literature whenever possible. Personality was measured using the validated 44-item BFI inventory developed by John *et al.* [10]. In contrast to the 240 item NEO-PI-R or the 60-item NEO-FFI [17], the BFI is advantageous due to its short and succinct phrasing, which is less time consuming for respondents. The behavioral constructs for mobile security were multi-item scales (see Appendix **Table 2**). All items were measured using a five-point Likert scale. In concordance with prior literature, subjective norm was regarded as a formative construct because it is comprised of causal items [36]. The items occur independently of the others within this construct [37]. All other items in the study were modeled as reflective. To increase content validity, measurement items for both formative and reflective constructs were based on validated prior literature. In addition, the complete questionnaire was pre-tested with nine faculty members and PhD students who were skilled in quantitative research methods.

4.3. Data Analysis and Results

Empirical data were analyzed using the component-based structural equation modeling approach of partial least squares (PLS) [38]. PLS is the preferred option in explorative studies of complex research relationships [38] and for studies during the early stages of theory building [3]. In addition, we chose PLS to handle the presence of a large number of measures and the combination of latent reflective and formative variables [39]. Model testing and measurement validation were conducted using SmartPLS (Version 2.0 M3).

Following the validation guidelines from Chin [38] and Straub *et al.* [40] for reflective measurement models, we made use of convergent validity, discriminant validity, and reliability. With regard to individual item reliability, the factor loadings of each item were assessed on its respective construct. Recommendations for threshold levels of item reliability range from a minimum loading of 0.4 [40] to ideally 0.707 as proposed by Chin [38]. The item reliability analysis of personality traits showed that some items had low factor loadings. This phenomenon is known in personality research [41]. Since we focus on the global dimensions rather than the single facets, removing items is appropriate. After purification, the lowest item loading on its respective underlying construct was 0.62 (agreeableness) so that every item was near the recommended ideal threshold of 0.707. To confirm internal consistency, composite reliability (CR) was measured. All constructs met the minimum threshold of 0.70 (lowest CR is PU with a CR of 0.79), which is considered to be sufficient [42]. To ensure convergent validity of constructs, average variance extracted (AVE) for each construct was above the minimum threshold of 0.50 (lowest AVE is extraversion with an AVE of 0.59). For adequate discriminant validity, the square root of the AVE for each construct exceeded the correlation values in the correlation matrix [42].

Regarding the formative measure, we first ensured the content validity by using validated past empirical studies. To ensure that multicollinearity was not present in this study, we used variance inflation factor (VIF) statistic. A VIF of ten or below is required [38]. Since the VIF value was 1.01, no multicollinearity could be observed. In addition, all weights of formative indicators were significant at $p < 0.01$ (lowest t-value 2.98).

5. Discussion

The aim of this study was to examine how personality traits influence the cognitive determinants of users' intention with respect to smartphone security measures. It was shown that personality traits are influential in determining core constructs of TPB and TAM. **Figure 2** provides the estimates of the path coefficients and a summary of the results of hypotheses. As predicted by TPB, TAM, and in consistence with our expectations and the results of prior studies in information security research (e.g. [4,8]), a smartphone user's intention is strongly influenced by the core constructs PU ($\beta = 0.329$; $p < 0.001$), SN ($\beta = 0.281$; $p < 0.001$), and PBC ($\beta = 0.395$; $p < 0.001$). In more detail, smartphone users' intentions to use security measures are mainly motivated by their beliefs about the usefulness and whether the use is under their control. The results also imply that social influence

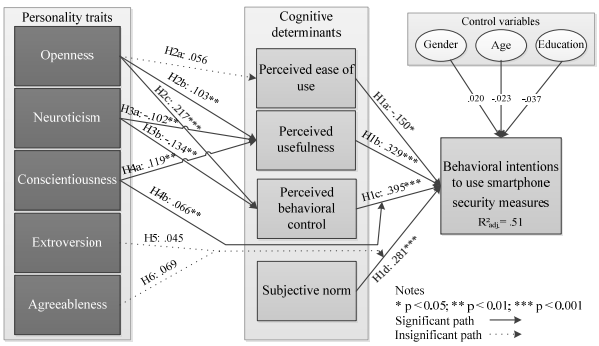

Figure 2. Results of PLS structural equation model analysis.

determines the intentions to use security measures. A smartphone user is likely to use security measures if she or he perceives that significant others are using the same security measure. Contrary to TAM, H1a is not supported. A negative significant influence of PEOU to INT is identified. Upon reflection, this result can be the phenomenon of other external variables, influencing the relationship between PEOU and INT. For example, Venkatesh and Bala [43] highlighted the sensitivity of potential moderators that influence the relationship between PEOU and INT. The authors found that experience moderated the effect of PEOU and INT such that the effect becomes weaker with an increase in user experience levels [43]. It is possible that the relationship between PEOU and INT might be more complex than a linear relationship. Overall the cognitive determinants accounted for a significant proportion of the variance in INT (R^2_{adj} = 0.51).

Further, the results of our study indicate that the cognitive determinants of security measures vary depending on different personality traits. More specifically, out of the nine hypothesized relationships between personality traits and cognitive determinants and behavioral intentions, six significant relationships were identified. Openness was hypothesized to have a positive relationship to PEOU, PU, and PBC. Due to the facets of, for example, a higher scope of awareness, open smartphone users are found to form positive beliefs about the usefulness of potential security measures. In addition, facets such as being intelligent and willingness to learn [19] make smartphone users believe in their own ability to use different security measures. A significant relationship between openness and PEOU could not be identified. As mentioned above, other external variables such as experience might influence the relationship between openness and PEOU. Devaraj *et al.* [8] pointed out that the relationship between openness and attitudinal constructs might be more complex than a simple linear relationship. The authors justified their argumentation by demonstrating that openness and attitudinal constructs were not significant, while a direct positive relationship to behavioral intention exists. Turning to neuroticism, the results indicate that neuroticism has a negative impact on PU and PBC. Prior research stated that neurotic individuals tend to avoid taking control of a situation; this research study confirms this relationship. Additionally, neurotic smartphone users are more skeptical and form negative beliefs towards the usefulness of a security measure and their own ability to take control of using a security measure. Turning to conscientiousness, both hypotheses are supported. These results are not surprising, since conscientiousness has been shown to be an important personality trait in information security research [1].

Agreeable and extraverted smartphone users are hypothesized to influence the relationship between SN and INT. In prior research, it was pointed out that in a situation that requires interpersonal interaction, both traits appear to show a high predictive validity [19]. However, prior research has shown that self-efficacy, or in the case of this study, PBC, eliminates the effect of extraversion on behavioral intention [31]. Therefore, a reason for H6 not being supported can be the strong impact of PBC on INT. Another reason can be the peculiarity of extravertsion with the desire to gain social status. Within the context of smartphone security measures, social pressure does not affect the social cues within this personality trait. On the other hand, agreeableness shows its facets in interpersonal interactions, especially in situations that involve helping and cooperating with others [19]. Social pressure to use security measures refers to the extent to which the use of a security measure is perceived as enhancing a smartphone user's image or status in a social system. Agreeableness may show its facets more in helping and supporting others. Agreeable smartphone users are more willing to help others, but may not necessarily feel compelled to use security measures because of social pressure.

6. Implications and Recommendations

This study makes theoretical and practical contributions to the emerging knowledge of behavioral issues in regard to the use of mobile security measures. Literature in information security investigated both personality and cognitive factors to explain different behaviors in each human being. With the exception of Devaraj *et al.* [8] and Nov and Ye [9], who based their work on TAM, research has not focused on understanding the main personal determinants of cognitive key factors that influence intended behavior. Further, to the best of our knowledge, this is the first study that combines personality traits and mediated cognitive factors to intended behavioral outcome in a mobile security context. Knowing that personality traits are stable over time, results indicate that cognitive factors about the overall acceptance of smartphone security measures are influenced by personality traits in different ways. Therefore, the current research demonstrates a more complete, integrated, and coherent view of the acceptance of security measures. These results can spur other researchers to examine personality traits together with other established behavioral models, such as general deterrence theory or protection motivation theory, in information security research.

On the more practical side, this study sheds light on different kinds of smartphone users and their cognitive processes that result in intended behavior. The applied cognitive factors are associated with intentions to use a security measure, and to actual use behavior. In the current debate of consumerization (e.g. [44]), organizations

can benefit from our findings that different kinds of individuals are likely to form positive attitudes and intentions towards security measures by developing preventative strategies. While personality traits are stable over time, cognitive factors such as beliefs about the perceived usefulness or perceived behavioral control can be directly enhanced. Practitioners should attempt to adapt these findings and design specified user training.

7. Limitations and Future Research

The study is subject to following limitations: First, as this study is based on a student sample of smartphone users, the results cannot be generalized to the entire smartphone user's population. The rationale for using student samples is explained in section 3.1 and has been evaluated to be appropriate for the purpose of this study. We encourage validation of our findings with other population segments. Further, despite the use of actual behavior, this study is based on self-reported information that measures behavioral intentions. Due to the sensitive context of security measures and the investigated object of smartphones, which can be seen as an object of privacy, it is difficult to obtain data about actual behavior. To focus more on the gap between behavioral intention and actual behavior, and to link that with the FFM, one option to alleviate this limitation is to use scenario techniques [26]. Providing broader information about hypothetical information security situations and indirectly asking about attitudes towards security measures might allow researchers to get a better impression of a smartphone user's true behavior. Further, respondents are from a German university. In regard to cross-national differences in personality, it is likely that smartphone users from other countries have different attitudes about or reactions to the protection of their smartphones. Future studies could integrate cultural differences by expanding into a more international context.

8. Conclusion

This paper presents a first attempt at investigating how personality traits of smartphone users affect cognitive determinants for the use of security measures. Recent studies have acknowledged the influence of personality traits on IS success outcome factors; however, incorporating personality traits from smartphone users' perspective into determinants of behavioral intention to use security measures have largely been ignored. Personality is measured by the FFM; the determinants of behaveioral intention are adapted from TPB and TAM, the latter is represented by PEOU and PU. Results indicate that personality traits influence smartphone security measures' usage. For example, openness, neuroticism, and conscientiousness are found to have a significant influence on smartphone users' beliefs towards the usefulness of a security measure. In addition, the core cognitive determinants of behavioral intentions are all found to significantly influence the intention to use security measures.

REFERENCES

[1] J. Shropshire, M. Warkentin, A. C. Johnston and M. B. Schmidt, "Personality and IT security: An Application of the Five-Factor Model," *Proceedings of the* 12*th Americas Conference on Information Systems*, *Acapulco* (*Mexico*), Acapulco, 4-6 August 2006, pp. 3443-3449.

[2] W. Wang, "How Personality Factors Affects Continuance Intention: An Empirical Investigation of Instant Messaging," *Proceedings of the* 14*th Pacific Asia Conference on Information Systems*, Taipei, 9-12 July 2010, p. 113.

[3] H. H. Teo, K. K. Wei and I. Benbasat, "Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective," *MIS Quarterly*, Vol. 27, No. 1, 2003, pp. 19-49.

[4] C. L. Anderson and R. Agarwal, "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Behavioral Intention," *MIS Quarterly*, Vol. 34, No. 4, 2010, pp. 613-643.

[5] B. Lebek, J. Uffen, M. Neumann, B. Hohler and M. H. Breitner, "Employees' Information Security Awareness and Behavior: A Literature Review," *Proceedings of the* 45*th Hawaii International Conference on System Science*, *Maui* (*USA*), Wailea, 7-10 January 2013, pp. 2978-2987.

[6] M. Fishbein and I. Ajzen, "Belief, Attitude, Intention and Behavior," John Wiley, New York, 1975.

[7] I. Ajzen, "Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, Vol. 50, No. 2, 1991, pp. 179-211. http://dx.doi.org/10.1016/0749-5978(91)90020-T

[8] S. Devaraj, R. F. Easley and J. M. Crant, "How Does Personalty Matter? Relating Five-Factor Model to Technology Acceptance and Use," *Information Systems Research*, Vol. 19, No. 1, 2008, pp. 93-115. http://dx.doi.org/10.1287/isre.1070.0153

[9] O. Nov and C. Ye, "Personality and Technology Acceptance: Personal Innovativeness in IT, Openness and Resistance to Change," *Proceedings of the* 41*st Hawaii International Conference on System Science*, *Big Island* (USA), Waikoloa, 7-10 January 2008, p. 448.

[10] O. P. John, E. M. Donahue and R. L. Kentle, "The Big Five Inventory—Version 4a und 54," Institute of Personality and Social Research, University of California, Berkeley, 1991.

[11] R. A. Botha, S. M. Furnell and N. L. Clarke, "From Desktop to Mobile: Examining the Security Experience," *Computer and Security*, Vol. 28, No. 3-4, 2009, pp. 130-137. http://dx.doi.org/10.1016/j.cose.2008.11.001

[12] Z. Tu and Y. Yuan, "Understanding User's Behaviours in Coping with Security Threat of Mobile Devices Loss and Theft," *Proceedings of the* 45*th Hawaii International Conference on System Science*, Maui, 4-7 January 2012, pp. 1393-1402.

[13] R. W. Smith and A. Pridgen, "STAAF: Scaling Android Application Analysis with a Modular Framework," *Proceedings of the* 45*th Hawaii International Conference on System Sciences*, Maui, 4-7 January 2012, pp. 5432-5440.

[14] J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse," *Information Systems Research*, Vol. 20, No. 1, 2009, pp. 79-98. http://dx.doi.org/10.1287/isre.1070.0160

[15] N. L. Clarke andS. M. Furnell, "Authentication of Users on Mobile Telephones—A Survey of Attitudes and Practices," *Computer & Security*, Vol. 24, No. 7, 2005, pp. 519-527. http://dx.doi.org/10.1016/j.cose.2005.08.003

[16] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer and S. Möller, "On the Need for Different Security Methods on Mobile Phones," *Proceedings of the* 13*th International Conference on Human Computer Interaction with Mobile Devices and Services*, Stockholm, 30 August-2 September 2011, pp. 465-473.

[17] P. Costa, R. McCrae and D. Dye, "Facet Scales for Agreeableness and Conscientiousness: A Revision of the NEO Personality Inventory," *Personality Individual Differences*, Vol. 9, No. 12, 1991, pp. 887-898. http://dx.doi.org/10.1016/0191-8869(91)90177-D

[18] G. W. Allport, "Pattern and Growth in Personality," Holt, Rinehart & Winston, New York, 1961.

[19] M. R. Barrick, M. K. Mount and T. A. Judge, "Personality and Performance at the Beginning of the New Millennium: What Do We Know and Where Do We Go Next?" *International Journal of Selection & Assessment*, Vol. 9, No. 1-2, 2001, pp. 9-29. http://dx.doi.org/10.1111/1468-2389.00160

[20] T. A. Judge, J. E. Bono, R. Ilies and M. W. Gerhardt, "Personality and Leadership: A Qualitative and Quantitative Review," *Journal of Applied Psychology*, Vol. 87, No. 4, 2002, pp. 765-780. http://dx.doi.org/10.1037/0021-9010.87.4.765

[21] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, Vol. 13, No. 3, 1989, pp. 319-339. http://dx.doi.org/10.2307/249008

[22] I. Junglas, N. Johnson and C. Spitzmüller, "Personality Traits and Concern of Privacy: An empirical Study in the Context of Location-Based Services," *European Journal of Information Systems*, Vol. 17, No. 4, 2008, pp. 387-402. http://dx.doi.org/10.1057/ejis.2008.29

[23] Y. Lee, K. A. Kozar and K. R. T. Larsen, "The Technology Acceptance Model: Past, Present, and Future," *Communications of the AIS*, Vol. 12, 2003, pp. 752-780.

[24] V. Venkatesh, M. G. Morris, G. B. Davis and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, Vol. 27, 3, 2003, pp. 425-478.

[25] R. Sharma and P. Yetton, "The Contingent Effects of Management Support and Task Interdependence on Successful IS Implementation," *MIS Quarterly*, Vol. 27, No. 4, 2003, pp. 533-556.

[26] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, Vol. 34, No. 3, 2010, pp. 523-548.

[27] S. Goswami, H. H. Teo and H. C. Chan, "Decision-Maker Mindfulness in IT Adoption: The Role of Informed Culture and Individual Personality," *Proceedings of the* 30*th International Conference on Information Systems*, Phoenix, 15-18 December 2009, p. 203.

[28] D. R. Compeau and C. A. Higgins, "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly*, Vol. 19, No. 2, 1995, pp. 189-211. http://dx.doi.org/10.2307/249688

[29] Q. Hu, T. Dinev, P. Hart and D. Cooke, "Top Management Championship and Individual Behavior towards Information Security: An Integrative Model," *Proceedings of the* 16*th European Conference on Information Systems*, *Galway*, 9-11 June 2008, pp. 1310-1321.

[30] G. Bansal, "Security Concerns in the Nomological Network of Trust and Big5: First Order vs. Second Order," *Proceedings of the* 32*nd International Conference on Information Systems*, Shanghai, 7 December 2011, Paper 9.

[31] J. C. McElroy, A. R. Hendrickson, A. M. Townsend and S. M. DeMarie, "Dispositional Factors in Internet Use: Personality versus Cognitive Styles," *MIS Quarterly*, Vol. 31, No. 4, 2007, pp. 809-820.

[32] A. R. Korukonda, "Differences that do Matter: A Dialectic Analysis of Individual Characteristics and Personality Dimensions Contributing to Computer Anxiety," *Computers in Human Behavior*, Vol. 23, No. 4, 2007, pp. 1921-1942. http://dx.doi.org/10.1016/j.chb.2006.02.003

[33] A. G. Kotulic and J. G. Clark, "Why There Aren't More Information Security Research Studies," *Information & Management*, Vol. 41, No. 5, 2004, pp. 597-607. http://dx.doi.org/10.1016/j.im.2003.08.001

[34] S. Okazaki, "What Do We Know About Mobile Internet Adopters? A Cluster Analysis," *Information and Management*, Vol. 43, No. 2, 2006, pp. 127-141. http://dx.doi.org/10.1016/j.im.2005.05.001

[35] H. Dai, A. F. Salam and R. King, "Service Convenience and Relational Exchange in Electronic Mediated Environment: An Empirical Investigation," *Proceedings of the* 29*th International Conference on Information Systems*, Paris, 14-17 December 2008, pp. 1-20.

[36] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviours: An Empirical Study," *MIS Quarterly*, Vol. 34, No. 3, 2010, pp. 549-566.

[37] C. B. Jarvis, S. B. MacKenzie and P. M. Podsakoff, "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *Journal of Consumer Research*, Vol. 30, No. 2, 2003, pp. 199-218. http://dx.doi.org/10.1086/376806

[38] W. W. Chin, "Issues and Opinion on Structural Equation Modeling," *MIS Quarterly*, Vol. 29, No. 3, 1998, pp. 7-16.

[39] S. Petter, D. Straub and A. Rai, "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly*, Vol. 31, No. 4, 2007, pp. 623-656.

[40] W. Straub, M. C. Boudreau and D. Gefen, "Validation

Guidelines for IS Positivist Research," *Communications of the AIS*, Vol. 13, No. 24, 2004, pp. 380-427.

[41] W. Renner, "A Psychometric Analysis of the NEO Five-Factor Inventory in an Austrian Sample," *Review of Psychology*, Vol. 9, No. 1, 2002, pp. 25-31.

[42] D. Gefen, D. W. Straub and M. C. Boudreau, "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the AIS*, Vol. 4, No. 7, 2000, pp. 1-80.

[43] V. Venkatesh and H. Bala, "Technology Acceptance Model 3 and a Research Agenda on Interventions," *Decision Sciences*, Vol. 39, No. 2, 2008, pp. 273-315. http://dx.doi.org/10.1111/j.1540-5915.2008.00192.x

[44] F. Weiß and J. M. Leimeister, "Consumerization-IT Innovations from the Consumer Market as a Challenge for Corporate IT," *Business and Information Systems Engineering*, Vol. 4, No. 6, 2012, pp. 363-366.

Appendix

Table 2. Questionnaire items.

Item	Measure (translated from German)
	Behavioral intention (e.g. Venkatesh *et al*., 2003; Davis, 1989; Ajzen, 1991; Anderson and Agarwal, 2010)
INT1	I intend to continuously engage in security measures for my smartphone
INT2	I will execute data-backups on my smartphone in intervals of less than 3 months
INT3	I plan to change my smartphone PIN-authentication in regular intervals
INT4	I intend to execute updates for firmware and apps in regular intervals
INT5	I intend to receive information about new security measures for my smartphone in the near future
	Perceived ease of use (e.g. Venkatesh, 2000; Venkatesh and Davis, 2000)
PEOU1	I think the enabling of security measures like PINs is easy for most people
PEOU2	I think most people execute regular updates of apps and firmware
PEOU3	I think with modern smartphones, most people can easily execute backups
PEOU4	A lot of expertise is needed to implement security measures on a smartphone
	Perceived usefulness (e.g. Venkatesh, 2000; Venkatesh and Davis, 2000)
PU1	I think PIN-authentication for my smartphone is fundamental
PU2	I would only use a lot of functions on my smartphone if I perceived my data to be safe
PU3	I consider data backups to be very important to effectively avoid data loss
	Subjective norm (e.g. Ajzen, 1991; Johnston and Warkentin, 2010; Venkatesh, 2003)
SN1	People in my closer environment think I should protect the data on my smartphone, for example via regularly backups
SN2	I know a lot of people who use PIN-authentication or similar security measures on their smartphone
SN3	People who influence my behavior use different security measures to protect their smartphones
	Perceived behavioral control (e.g. Compeau and Higgins, 1995)
PBC1	It is easy for me to enable PIN-authentication on my smarthphone
PBC2	I always need someone to assist when I want to change security settings on my smartphone
PBC3	Constant updates for apps and firmware are easy for me
PBC4	Executing data backups is entirely under my control

