PERSONALITY TRAITS AND INFORMATION SECURITY MANAGEMENT: AN EMPIRICAL STUDY OF INFORMATION SECURITY EXECUTIVES

Completed Research Paper

Jörg Uffen
Information Systems Institute
Leibniz Universität Hannover
uffen@iwi.uni-hannover.de

Nadine Guhr
Information Systems Institute
Leibniz Universität Hannover
guhr@iwi.uni-hannover.de

Michael H. Breitner
Information Systems Institute
Leibniz Universität Hannover
breitner@iwi.uni-hannover.de

Abstract

Executives' behavior causes potential information security management risks and has a direct influence on the security level of information systems and management. This behavior depends on personality traits and other cognitive factors. First, a comprehensive literature review and a status quo analysis are presented. We consider the constructs of the Five Factor Model (FFM) as influence factors for attitudes towards technical and non-technical dimensions of information security management. Then, the hypothesized relationships are validated using empirical data from 174 information security executives. The results suggest that multiple facets of an information security executive's personality have a significant effect on his or her attitude towards selected information security management activities. For example, conscientiousness is positively related to a person's attitude towards the technical and organizational activities of information security. From these findings, theoretical and practical implications and recommendations are discussed.

Keywords: Personality traits, Five Factor Model, information security executives, attitude, Theory of Planned Behavior

Introduction

Security threats can have dire consequences, including loss of prestige and credibility, corporate liability, and monetary damage (Bulgurcu et al. 2010). Research studies emphasize management's increasing concerns about the protection of organizational information assets (Straub and Welke 1998; Taylor 2006). Hence, an important issue in today's organizations is to determine how to create efficient and sustainable information security. The way management – or information security executives – cope with potential information security risks and react in different situations varies from individual to individual and depends on personality and other cognitive factors (Straub and Welke 1998; Vroom and von Solms 2004). Individual management differences have become an important area of focus in information security research. For example, Sharma and Yetton (2003) investigated the positive influence of management on employee's cognitive beliefs, attitudes, and behavioral patterns when dealing with information security. Ashenden (2008) emphasized the need for management soft skills to effectively change organizational culture and to improve communication between end-users, information security executives, and senior managers. And Stanton et al. (2005) highlighted the fact that effective security organization and leadership help to improve the security environment for end-user compliance.

The purpose of this paper is to investigate how individual differences between information security executives affect holistic information security management within organizations and companies. Individual differences are measured using the Five Factor Model (FFM) (Costa and McCrae 1991). The way an information security executive perceives holistic information security management is measured by his or her attitude towards technical and six non-technical dimensions of information security – strategy, organization, human, culture, compliance, and economy.

We examine the relationship between executives' personality and information security for several reasons. First, personality traits have been shown to be an important instrument in IS literature, because they emphasize an individual's cognitive processes, attitudes, and behaviors (Junglas et al. 2008). Yet a number of studies have shed some light on the individual differences in the IS domain (e.g. Lee and Larson 2009; Benlian and Hess 2010; McElroy et al. 2007). In the information security field, target subjects of previous studies were limited to users or employees (e.g. Shropshire et al. 2006). Incorporating the FFM from the executives' perspective has largely been ignored. Second, researchers have called for more rigorous empirical research to advance sustainability and efficiency in the information security domain (e.g. Kotulic and Clark 2004; Zhao et al. 2009). The role and responsibility of executives in information security have been shown to be main predictors of success (e.g. McFadzean et al. 2007; Straub and Welke 1998). Third, focusing on the problem from a holistic, multidimensional rather than a simple, one-dimensional information security management approach allows us to examine and evaluate information security phenomena from the individual executives' perspective. Personality traits can illustrate how individual differences determine the strength of a person's attitude towards holistic information security management. In this emerging research context, we believe that a global focus is beneficial for researchers and practitioners alike. This paper makes a theoretical contribution by conceptualizing that executives' actions and decisions are essentially driven by their personalities. We explore the following research question by testing an integrated personality model:

Which personality traits of an information security executive have a major influence on technical and non-technical components of information security management?

This paper is structured as follows: first, we provide a theoretical basis and outline the identified research gap. Because of the relevance of structural equation modeling (SEM) in this research stream, a comprehensive overview of relevant literature is presented, followed by a description of the research design. After presenting the model development and analysis, we report the results of our field study of information security executives who are involved in information security management. Following the discussion of results, we conclude with a discussion of implications for research and practice, limitations and an outlook for future research.

Foundations, conceptual basis, and hypotheses generation

Information security

Several researchers highlight the importance of a holistic, multidimensional information security management approach to securing technology, people, processes, and other organizational factors (Da Veiga and Eloff 2007; Hu et al. 2006; May and Dhillon 2010). Information security management is affected by multiple distinctive dimensions. Researchers are paying more attention to incorporating several dimensions, such as social and technical issues, into information security management models, frameworks, and architectures (May and Dhillon 2010). For example, Torres et al. (2006) discussed 12 critical success factors that were qualitatively identified from a set of 76 indicators, and which were valuable for measuring information security levels. May and Dhillon (2010) conceptualized a holistic information security management model that is meta-theoretically based on the theory of semiotics. The authors elaborated that the human and technical dimensions of information security management can be brought together via six layers, the output of which provides information for other layers in a collaborative manner. In their review, Zafar and Clark (2009) presented an information security capability reference model that is based on nine dimensions – governance, privacy, threat mitigation, transaction and data integrity, identity and access management, application security, physical security, personnel security, and information security economics. In addition, national and international organizations issued fundamental best-practices, guidelines and standards, for example 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 800-39 that provide recommendations regarding the implementation and management of information security issues. These standards indicate that information security must be managed using a holistic, multidisciplinary approach, cutting horizontally across units within and across organizational boundaries along the entire value chain.

In information security research, one limitation is that there is no generally accepted model or framework with coherent dimensions or labels (Kritzinger and Smith 2008; May and Dhillon 2010). Due to lack of awareness and expertise, complex and extensive processes, and high cost, organizations often face difficulties in managing a holistic information security concept (Eloff and Eloff 2005). In addition, Siponen and Willison (2009) noted that standards or guidelines are generic in scope and do not focus on the different security requirements in organizations.

To get a valid theoretical foundation, we use the perspectives of prior work of Da Veiga and Eloff (2007), Kritzinger and Smith (2008), Ma and Pearson (2005), Saleh et al. (2007) and Werlinger et al. (2010) in combination with the above-mentioned national and international information security standards. Security management approaches can generally be divided into two essential components – technical and non-technical information security components (Kritzinger and Smith 2008). The former addresses the technical dimension of information security management that enables the technology services and applications. The latter includes human-related issues such as user awareness, organizational issues such as top-management support or leadership, ethical and cultural aspects, economic factors, and compliance, including legislative, regulatory, contractual requirements, as well as internal policies and procedures (e.g. Da Veiga and Eloff 2007; Werlinger et al. 2010; Saleh et al. 2007). For our purposes, strategic, human, organizational, and compliance information security dimensions are considered as non-technical component. Further, in contrast to Saleh et al. (2007), who incorporated ISO 17799:2005 into a framework with the basic dimensions of strategy, organization, people, and environment as non-technical components, we divided the latter into cultural and economic dimensions due to their high relevance to information security research (e.g. Cavusoglu et al. 2005; Da Veiga and Eloff 2007; Ruighaver et al. 2007). In information security research, the cultural dimension is separated from the human dimension. While the human dimension includes issues relating to security education, training, awareness programs and computer monitoring (e.g. D'Arcy et al. 2008; Bulgurcu et al. 2010), cultural dimensions are based on assumptions about accepted and encouraged aspects such as attitudes, norms and shared expectations, which are seen as an accepted type of employee conduct (Ruighaver et al. 2007). Culture differs from the human factor because humans are regarded as a whole within the organizational context instead of as an individual who guides actions like security training methods (Vroom and von Solms 2004). The economic dimension of information security management takes financial and non-financial factors into account, such as budgetary restrictions, cost-efficiency of information security investments, and timing of

implementation (Cavusoglu et al. 2005; Park et al. 2010). However, in this paper, holistic information security management aims to maximize the number of prevented and deterred security breaches (D'Arcy et al. 2009) by the management of an efficient set of non-technical components, represented by strategy (STRAT), human (HUM), organization (ORG), compliance (COM), culture (CULT) and economic (ECO) dimensions, and technical (TECH) component.

Not only are executives responsible for communicating an acceptable security culture, compliance and exhibiting information security behavior (Da Veiga and Eloff 2007), they have to focus a multi-disciplinary view (Theoharidou et al. 2005). Therefore, an executive's key attributes that are valuable for information security go beyond simply securing information assets. They must also be able to integrate organizational security needs into business goals and objectives (Whitten 2008). As such, executives have to consider all dimensions that are part of information security management. But the way individuals act in different situations depends on personality and varies from person to person (Vroom and von Solms 2004). Based on the theoretical conceptualization of holistic information security management, there appears to be some sort of relationship between an executive's personality and his or her attitude towards a holistic information security management approach.

Personality and the role of personality in information security research

Individual differences play a ubiquitous role in the IS domain. Researchers have incorporated related cognitive and personality-related variables into various IS success outcome models. An executive's perceptions of security risks have a strong influence on the decision-making process (Straub und Welke 1998; Taylor 2006). There is also evidence that an information security executive's sensitivity towards security activities and advanced security software is associated with a higher perceived effectiveness of information security (Straub and Welke 1998; Krankanhalli et al. 2003). However, personality psychologists use classification systems that summarize individual differences in personality into fundamental facets of each human being. These traits determine cognitive and behavioral patterns that remain more or less stable across situations (Costa et al. 1991). 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" (Allport 1961, p. 28). The most frequently used taxonomy in personality research is the FFM (Barrick et al. 2001). The FFM, a parsimonious and comprehensive model of personality, became widely accepted in personality research because its validity was verified by multiple empirical studies (McCrae and John 1992). Despite criticism of the number and labels of FFM factors (e.g. Barrick et al. 2001; Eysenck 1992), a number of beneficial properties, that are associated with the use of the FFM are stability, presence, and collective appreciation (Costa et al. 1991). The five broad constructs are generally referred to conscientiousness (CON), agreeableness (AGREE), extraversion (EXTRA), openness (OPEN) and emotional stability (EMO_STAB) (e.g. Costa et al. 1991; Digman 1990).

Empirical studies that focus on the human factor with regard to information security tend to emphasize user or employee behavior (Bulgurcu et al. 2010). These studies assessed related topics by presenting preventive strategies in an end-user context in terms of a user's or employee's contribution to individual mistakes, inaccuracies, or faults in order to improve information security. For example, in their study, Shropshire et al. (2006) proposed a link between two FFM criteria and information security compliance behaviors. Results establish that agreeableness and conscientiousness are strongly connected with an end-user's intention to comply with an organizational security policy. Bansal (2011) examined the relation of FFM and concerns of security and privacy on websites. Results indicate that neuroticism, conscientiousness and extraversion are positively related with concerns for security. Personality traits of agreeableness and openness are significantly associated with concern for privacy. In the same context, Junglas et al. (2008) showed that personality traits impact concern for privacy in location-based services. Using protection motivation theory, the authors investigated whether agreeableness, conscientiousness, and openness affect the concern for privacy.

Although the studies provide the groundwork for the current analysis, they do not quantify the relation between information security management dimensions from the perspective of executives' personalities. Empirical studies that address an executive's personality when assessing the impact on information security are still lacking. By focusing on personality traits of information security executives, this paper provides a more global lens for analyzing the impact of personality traits on holistic information security management components. With regard to the research objective, we developed hypotheses (H) about the

influence of an information security executive's personality traits on the above-mentioned technical and non-technical components of information security management.

Rationale and hypotheses generation

Personality research shows that personality traits vary in their respective relevance but are resistant to transformation (Junglas et al. 2008). Prior meta-analytic evidence has demonstrated that some FFM traits are more relevant in explaining different factors of behavior (Barrick et al. 2001). For example, individuals with higher scores on extraversion are related with greater training proficiency (Hough 1992; Barrick et al. 2001), while agreeableness is helpful for tasks that require considerable interpersonal interaction (Mount et al. 1998). Both traits are characterized by social interaction factors in human beings. Consequently, agreeableness and extraversion are judged on the information security dimensions that incorporate interpersonal interaction. In contrast, openness is considered to be important in studies that focus less on interpersonal interaction (Mount et al. 1998). Empirical evidence has shown that individuals who have less emotional stability tend to be more risk-averse (Lauriola and Levin 2001) and less goal-oriented (Judge and Ilies 2002). This is expected to be an indicator of their attitude toward the long-term and the economic view. Conscientiousness, with its facets of dutifulness and a need for achievement, is a fundamental trait of intrinsic motivation and a high level of job performance (Barrick et al. 2001; Devaraj et al. 2008). Because of these facets, conscientiousness is more likely to be relevant in studies that attempt to investigate multiple factors of performance. Based upon these findings it is concluded that due to the variety of information security components, specific personality traits are hypothesized to be related to some, but not every one of the technical and non-technical information security management components. A hypothesized relationship is relevant when it is appropriate, and is grounded in and supported by theoretical and empirical research studies. Further, in consideration of our research objectives, we focus only on the five global dimensions of FFM instead of on their specific detailed facets.

Conscientiousness, a personality trait that is associated with purposeful planning and persistence, is one of the most important traits within the research of information security behavior (Hu et al. 2008; Shropshire et al. 2006). Prior research suggested a significant positive relationship between conscientiousness and general job performance (Barrick et al. 2001). Further, Goswami et al. (2009) emphasized the strong influence that conscientiousness has on mindfulness in IT innovations. Bansal (2011) demonstrated that conscientiousness is positively associated with security concerns. Information security management, with its changing requirements and challenges, requires a high level of attention and professionalism in complex situations (Torres et al. 2006). Traits such as dutifulness, persistence, and self-discipline are important characteristics that support an executive in his or her attempts to completely understand complex situations (Barrick et al. 2001). Planning, organizing, and prioritizing tasks under the prerequisite of ensuring compliance with internal and external requirements is essential for executives when focusing holistic information security management. One goal in the information security environment is persisting when faced with obstacles. Together with working hard, these facets are positively associated with conscientiousness (Holland et al. 1993). Therefore we postulate that information security executives with a higher degree of conscientiousness tend to react more carefully (Li et al. 2006), taking organizational requirements into consideration and working to improve information security across the technical and non-technical information security management components, the latter represented by CULT, HUM, ORG, COM, STRAT and ECO dimensions.

More specifically, to cultivate an adequate level of information security, users or employees need to be trained on how to behave in accordance with the security requirements (Da Veiga and Eloff 2007). Considering the cognitive learning processes and the behavioral outcomes of users and employees is critical in performing security awareness trainings in organizations, for example (Warkentin et al. 2011). Due to its facets, we expect that conscientiousness information security executives will have a stronger desire to face the human information security management dimension (H1c). Sensitive information is more and more protected by regulatory requirements. Information security executives have a legal mandate to determine policies and procedures for security compliant behavior (Warkentin et al. 2011). Conscientiousness is closely related to an intrinsic desire to abide by rules and follow policies (Hu et al. 2008). Thus, we postulate that conscientiousness is positively related to the compliance (H1e) dimension of information security management. From a strategic perspective, information security executives have to design policies and procedures in a way that security compliant behavior becomes part of users' or

employees' every day jobs in an accepted and encouraged way (Da Veiga and Eloff 2007). Conscientious individuals are found to work methodologically and tend to be well organized, as well as being more rule-bound (Costa et al. 1991), and are expected to form positive attitudes towards the cultural dimension of information security management (H1b). Together with the facets of competence and foresight, we hypothesize a positive relation between conscientiousness and the strategic (H1f) and cultural (H1b) dimensions of information security management. Further, achieving these requirements and the organizational objectives require well established coordination and leadership skills (Whitten 2008). Barrick et al. (2001) emphasized that conscientiousness individuals show a tendency to keep things well organized. We hypothesize that conscientiousness is positively related to organizational information security management dimension (H1d). Individuals who are high in conscientiousness strive for efficiency, accuracy and are more likely to ruminate over things (Costa et al. 1991). Adopting multiple technical countermeasures that are valuable in different situations and do not negatively affect users or employees in their daily work processes require precise and well organized work. Conscientiousness information security executives try to carefully consider budgetary restrictions while emphasizing technical countermeasures. These challenges shape both the economic (H1g) and technical (H1a) dimensions of information security management and are expected to be positively related. Thus, conscientiousness is hypothesized to be positively associated with the seven dimensions of information security management.

H¹: Conscientiousness is positively associated with the attitude towards technical and non-technical dimensions of information security management (H1a-H1g).

Openness is associated with creativity, intelligence, receptiveness to new ideas, and imaginativeness. Associated with various cognitive skills and abilities in individuals, openness is the motivational tendency to reflect on ideas, critically examine information, and solve puzzles (Goswami et al. 2009). Despite meta-analytic results that indicate that openness is not relevant to many work criteria (Barrick et al. 2001), these facets are quintessential aspects of information security management. Mindfulness, and in the same context, cognitively differentiated interpretation of information in multiple scenarios, is positively associated to openness in various situations (e.g. Goswami et al. 2009). Translated into the information security management context, the ability to face multiple challenges simultaneously and be receptive to new - but also to critically examine existing - ideas and information leads to more efficient actions and decisions if there is a security incident. Information security executives who are open are expected to be more sensitive to and make better sense of available information in a security breach situation, for example. As a result of such awareness, openness to innovation is expected to affect an information security executive's attitude towards both technical (H2a) and strategic information security dimensions (H2c).

Further, a parallel can be drawn to the attitude towards established controls and practices that must be critically examined regularly. Since rapid change and diversity are now the norm in the information security context, critical assessment and permanent monitoring processes have become key elements of an information security executive's tasks (Whitten 2008). Owing to a broader life experience, openness leads to a broader and deeper scope of awareness (Junglas et al. 2008) and more breadth-, and depth-minded thinking (Costa and McCrae 1992). Due to the nature of permanent monitoring processes, information security executives must be sensitive and broad-minded in order to scan and detect irregularities and peculiarities. In addition, those who have a high level of openness seek out new information (McCrae and Costa 1999). These facets are expected to lead to positive attitudes towards the critical assessment of the status quo in established controls and practices. Hence, we hypothesize that openness positively influences an information security executive's attitude towards the compliance dimension of information security management (H2b). Due to its general facets and its context, openness is not a useful predictor for dimensions with interpersonal interactions or an economic focus. Our hypothesis about this is as follows:

H²: Openness is positively associated with the attitude towards technical (H2a), compliance (H2b), and strategic (H2c) dimensions of information security management.

Extraverted individuals are characterized as being positive emotional, ambitious, energetic and dominant in social situations. 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 (McCrae and Costa 1999). Extraversion has been shown to lead to better performance

in tasks that require interpersonal interaction (Mount et al. 1998; Mount et al. 2005). Further, meta-analytic results indicate that extraversion is a useful predictor of management performance (Barrick et al. 2001) and leadership for effective team performance (Pierce and Hansen 2008). Extraverted individuals want to establish and maintain a favorable social status (Devaraj et al. 2008). Hence, in accordance to these findings, executives who are highly extraverted will develop positive attitudes to those information security dimensions that include the human component. To be precise, information security executives must be able to interact with a wide range of stakeholders across different organizational functions (Ashenden 2008), for example in terms of a information security awareness training (Bulgurucu et al. 2010; D'Arcy et al. 2009). Continuous proactive external and internal information procurement about current information security breaches, potential risks, and federal legislation and communication through different channels are a prerequisite to performing the job well (Whitten 2008). Therefore, establishing information security depends on effective communication with end users, team members and higher management levels (Ashenden 2008). Given the importance of interpersonal interaction in the context of information security and since this trait is associated with being outgoing, social, active, and talkative, it is expected that information security executives who are highly extraverted are more likely to have a positive attitude towards the dimensions with social and interpersonal interaction. These are represented by the human (H3a) and organizational (H3b) information security management dimensions.

H3: Extraversion of information security executives is positively associated with the attitude towards the human (H3a) and organizational (H3b) dimensions of information security management.

Research results suggest that agreeableness, like extraversion, is positively related to jobs that involve considerable interpersonal interaction, especially in job tasks when interaction involves helping and cooperating with others (Barrick et al. 2001). According to its facets, agreeableness is the trait that implies cooperating, nurturing other individuals (Barrick et al. 2001), and the ability to engage in teamwork (Mount et al. 1998). Empirical evidence indicates a positive effect of agreeableness on perceived team effectiveness (Pierce and Hansen 2008). The relation of agreeableness to information security is expected to be more likely related to an executive's attitude towards information security management dimensions when those dimensions involve cooperating, collaborating, and helping others. When faced with human challenges in information security (Ashenden 2008), executives who score high in agreeableness are expected to more likely empathize with end-users or team members (H4a) by being helpful with end user security problems. This information security dimension allows association with others and information security executives can make use of their considerate, likable, and helpful personalities. In addition, the required skills for information security executives, soft skills, the ability to sell security, and the management of relationships (Ashenden 2008) are aligned with agreeableness. Since organizational information security factors involve tasks such as leadership and coordination of teams or communication with a higher management level, agreeable information security executives will form positive attitudes towards this dimension. Thus, we hypothesize that the attitude towards organizational information security management dimension and the personality trait of agreeableness are positively associated with one another (H4b).

H4: Agreeableness is positively associated with attitude towards the human (H4a) and organizational (H4b) dimensions of information security management.

Previous studies highlighted emotional stability, the counterpart of neuroticism, as a valid predictor of job performance (Barrick et al. 2001) that has a positive effect on project outcome (Bedingfield and Thal 2008). Emotional stability is characterized by a lack of anxiety, pessimism, hostility, and personal insecurity. Unlike those who are emotionally stable, individuals who are neurotic are more risk averse (Lauriola and Levin 2001) and are shown to be less suited to higher level jobs that are more complex and stressful (Spector et al. 1995). Owing to the facets of emotional stability like a lack of pessimism and a tendency not to worry (McCrae and Costa 1999), we expect emotional stability to be related to technical, strategic, and economic dimension of information security management. For example, in information security management, risky situations require sophisticated reactions that are not premature (Karahanna and Watson 2006). Information security executives must make well-founded and balanced security investment decisions, but they must also fulfill the organizational information security requirements (Cavusoglu et al. 2005). Pessimism, or being worried, might lead to negative attitudes towards the economic dimension (H5a), which might in turn lead to inefficient strategic security management decisions.

Further, information security executives must understand business priorities, opportunities, and needs, and they must be able to critically examine the current implementation status in order to strategically protect organizational information (Smaltz et al. 2006). Emotionally stable information security executives are expected to identify changing security conditions and skeptically examine the current technical information security implementation and stability status. In this field, research has shown that emotionally stable individuals are likely to view innovative technical advances in their job as helpful and important (Devaraj et al. 2008). Thus, we hypothesize that emotionally stable information security executives will have positive attitudes towards the technical (H5c) and strategic (H5b) dimensions of information security management.

H5: Emotional stability is positively associated with the attitude towards economic (H5a), strategic (H5b) and technical (H5c) dimensions of information security management.

Research design and methodology

Explorative data collection procedures

Acknowledging the challenges associated with gaining acceptable empirical data in the critical domain of information security (Kotulic and Clark 2004), we chose the survey methodology to collect empirical data and to test the revised model statistically. We used two approaches to collecting empirical data. First, we used online networking websites with an exclusively professional focus (Xing, CIO, ITHeads) from which we identified 889 possible participants. We contacted information security executives, for example Chief Information Security Officers, from German-speaking countries via private messaging or email. We explicitly limited the survey to a national sample due to underlying cultural differences or different national regulatory requirements, which might cause different attitudes towards specific dimensions of information security management. When selecting participants, the authors did not focus on any particular businesses or industries to ensure that results were generally applicable. Second, in order to increase attention to our study, we used seven closed groups from the professional networks and solicited participation. Each closed group was selected based on its contextual focus on information security and was reviewed due to its professionalism.

Table 1. Sample demographics

Company size – # of employees (N=146)	**Frequency**	**Percentage**	**Industry (N=162)**	**Frequency**	**Percentage**
less than 50	24	14,7	Consulting	14	8,6
between 50 and 100	12	7,4	Manufacturing	14	8,6
between 100 and 250	16	9,8	Government	13	8,0
between 250 and 500	10	6,1	Telecommunication	11	6,8
between 500 and 1000	23	14,1	Health Care	10	6,2
between 1000 and 5000	32	19,6	Media	9	5,6
More than 5000	29	28,2	Education	8	4,9
Respondent's age (N=170)			Finance	8	4,9
From 20 to 30	6	3,5	Transport	8	4,9
From 30 to 40	40	23,5	Energy	6	3,7
From 40 to 50	73	42,9	Chemistry	6	3,7
From 50 to 60	44	25,9	Others	55	34,0
61 and above	7	4,1			
Involvement in information security (N=169)			**Respondent's educational level (N=163)**		
Directly involved	123	72,8	PhD	21	12,9
Indirectly involved	43	25,4	Diploma/ Master	101	62,0
Not involved at all	3	1,8	Others	41	25,2

Participation was voluntary, but was motivated by a promise to share the results. Due to the critical information being shared in the survey, participants were assured that their responses would be treated with anonymity and confidentiality, because the survey was hosted using a university-based survey tool in a secure environment. All questionnaires were completed with a web-based survey. Of the 889 preselected participants, 174 responses could be considered reliable, yielding a reasonable response rate of more than 19%. The response rate is acceptable given the nature of the study and the profile of the target group. From these, 158 respondents were directly contacted via one of the above-mentioned networks. The final sample frame comprised 154 male and 20 females. A summary of the demographic characteristics of respondents is provided in Table 1.

Operationalization of research variables and instrumentation

The items for constructs were adapted with the help of validated items from literature whenever possible. Personality was measured using the 60-item NEO-FFI format by Costa and McCrae (1992). Prior research suggested that the NEO-FFI is a reliable and valid instrument for FFM measurement (Barrick et al. 2001; Costa and McCrae 1992). The information security management constructs were developed and shaped by the literature, particularly by studies from Ma and Pearson (2005), Saleh et al. (2007), and Werlinger et al. (2008). Those studies and their related measures were developed with the help of international information security management standards and have been shown to be valid. Some new items are necessary to measure the different dimensions of information security management. The 33 items that represent the seven dimensions and constitute the attitude to a holistic information security management approach were included in the survey. As shown in several research studies and based on the Theory of Planned Behavior (TPB), a person's attitude towards a specific topic determines the intention of a specific action (e.g. Bulgurucu et al. 2010; Shropshire et al. 2006; Svendsen et al. 2011). In addition to our research objective, we postulate that an information security executive's attitude towards the technical and non-technical components of information security management influences his or her intention to apply information security holistically in daily job tasks.

Constructs with multiple items were measured using a five-point Likert scale, which ranged from "strongly disagree" to "strongly agree". To increase content validity, the questionnaire was pre-tested with five local IS managers and six faculty members – two with a psychological background and three with an information security background. Based on their feedback, we modified several items, especially in their wording. Afterwards, the questionnaire was discussed and verified with 12 other experts (eight faculty members and four IS managers). Measuring items are provided in the Appendix (Table 3).

Analysis methods and results

Due to the large number of items in the questionnaire, a factor analysis was conducted as a dimensional reduction method. The factor analysis was conducted using varimax rotation as the extraction method. The indicators are identified based on an eigenvalue that is greater than one. The total number of items was reduced based on the seven constructs: CULT, ECO, STRAT, COM, ORG, HUM and TECH, with a total of 33 indicators, which were identified in the literature review. These constructs were expected to influence the intention to manage information security in a holistic context (INFO_SEC) with a total of six indicators (see Appendix Table 3).

Empirical data was analyzed via SEM. SEM provides the researchers with the flexibility to model a relationship among criterion variables and multiple predictors, such as model errors in measurements for observed variables, to design unobservable latent variables, and statistically test a priori theoretical and measurement assumptions against empirical data (Chin 1998). Measurement validation and model testing were conducted using SmartPLS (Partial Least Squares) version 2.0.M3, a variance analytical SEM technique that utilizes a component-based approach to estimation. It is advantageous when the research model has a variety of indicators, is relatively complex, and the measures are not well established (Fornell and Bookstein 1982). PLS does not impose a normality requirement on the data and can handle both reflective and formative constructs, both of which are used in this study (Sun 2012; Wetzels et al. 2009).

The measurement model analyzed the relationship between the latent constructs and their associated indicators, also known as items or measures. In the course of operationalization, it is important to distinguish between reflective and formative measurement models because constructs in SEMs are not

inherently reflective or formative, which clearly differ with regard to their basic premises. Instead, constructs can be modeled with either reflective or formative indicators (MacKenzie et al. 2011). In contrast to formative constructs, reflective constructs have observed measures that are affected by an underlying, unobservable, latent construct (MacCallum and Browne 1993; Petter et al. 2007). In IS literature, reflective constructs are used for personality traits, where the unobservable can be considered as giving "rise to something observed" (Haenlein and Kaplan 2004). Therefore, we conceptualize the personality traits CON, OPEN, EXTRA, AGREE, and EMO_STAB as being reflective, because of the direction of the causality, the interchangeability of the indicators, the covariation among the indicators, and the nomological net of the constructs, which should not differ (Petter et al. 2007).

Constructs are the basic elements of a theory. We therefore captured the entire domain of the constructs and decided at the theoretical level whether the constructs in the field of information security management are formative or reflective to ensure content validity. After examining the relationship between each indicator and the construct in the field of information security management, we determined the overall constructs to be formative. In formative constructs the indicators define the characteristics of and changes in the underlying construct (Bagozzi 2011; Diamantopoulos 2011). They are also known as causal indicators and reflect the idea that "[...] indicators could be viewed as causing rather than being caused by the latent variable measured by indicators" (MacCallum and Browne 1993). Formative indicators are used to minimize residuals in the structural relationship (Petter et al. 2007) and to minimize "the trace of the residual variances in the 'inner' (structural) equation" (Fornell and Bookstein 1982). Internal reliability and consistency is irrelevant in case of formative constructs because measures are examining different facets of the construct (Petter et al. 2007).

First, the reflective constructs were analyzed. In this context, we examined the composite reliability, item reliability, and the convergent and discriminate validity. To ensure item reliability, we examined the loadings of each item to their respective underlying personality construct. Acceptable indicator loadings are recommended to be above at least 0.6 and ideally above the threshold of 0.707, indicating that at least 50 percent of the variance is shared with the respective construct (Chin 1998). The item reliability analysis of the personality traits shows that some indicators had low factor loadings. In personality research, low factor loadings are not unusual (Krishnan et al. 2010; Renner 2002). In consideration of our research objective, which focuses on the global dimensions and rather on its specific facets, removing indicators is appropriate. After purification, the remaining factor loadings of all indicators ranged from minimum 0.715 to 0.929, demonstrating that indicators are reliable for further analysis. All indicator loadings of personality traits are significant at $p < 0.001$. The composite reliability (also known as internal consistency reliability-ICR) is similar to Cronbach's alpha and measures its internal consistence, except that the latter presumes, a priori, that each indicator of a construct contributes equally (i.e. the loadings are set to unity) (Chin 1998; Fornell and Larcker 1981). Fornell and Lacker (1981) argued that their measure is superior to Cronbach's alpha because it uses the actual item loadings obtained within the nomological network to calculate internal consistency reliability. This measure, which is unaffected by scale length, is more general than Cronbach's alpha, but the interpretation of the values obtained is similar and the guidelines offered by Nunnally (1978) can be adopted (Howell and Avolio 1993). ICR should be 0.70 or higher (Diamantopoulos et al. 2008). The value is above the threshold, so that the internal consistency reliability is given. Convergent and discriminant validity was assessed by the average variance extracted (AVE). AVE represents the overall amount of variance in the indicators that was accounted by the latent construct. The reported values provide evidence of discriminant and convergent validity, since the AVE is well above the recommended level of 0.50 (Bhattacherjee and Premkumar 2004). The AVE values for all constructs in this model are higher than the recommended threshold value of 0.50 (smallest AVE: 0.565), suggesting the convergent validity of the scale (Bhattacherjee and Premkumar 2004). The Kaiser-Meyer-Olkin (KMO) criterion should be at least 0.5 (Chin 1998; Fishbein and Ajzen 1975; Streiner 2003). Here the KMO criterion is higher than the recommended threshold for the whole reflective measurement models. Overall, the evidence of reliability, convergent validity, and discriminant validity indicates that the measurement model is appropriate for testing the structural model at a subsequent stage.

The quality criteria for the formative measurement model are represented by the reliability and validity values in Table 2. At the indicator level, it is obligatory to test for multicollinearity, which illustrates whether and to what degree the items are mutually linearly dependent. But in particular, the concept of reliability has no significant meaning when formative models are employed. Thus, the importance of

reliability decreases, while the significance of assessing validity increases (Diamantopoulos 2011). The variance inflation factor (VIF) is equal to one and should not be greater than ten, as this might indicate the presence of harmful multicollinearity. In this study, multicollinearity did not pose a problem. The maximum VIF was far below the common threshold of ten and even below the conservative VIF threshold of 3.3 (Diamantopoulos and Siguaw 2006). Another important aspect is to test communality as validity criteria. As a rule of thumb, communality with a value of 0.9 or smaller may imply discriminant validity. Thus, it can be said that the quality criteria of the formative constructs are met on all levels.

Table 2. Quality criteria formative measurement model

Construct	CULT	TECH	HUM	ORG	STRAT	ECO	COM	INFO_SEC
Multicollinearity ($VIF^a \leq 10$)*	1.101	1.109	1.038	1.115	1.069	1.032	1.123	1.109
Communality (Comm. <0.9)**	0.269	0.438	0.501	0.235	0.357	0.576	0.181	0.229

*Threshold – [a]VIF (Variance inflation factor); **Threshold Communality

To receive valid results, the bootstrapping resampling procedure was used with 1000 resamples to obtain estimates of standard errors for testing the statistical significance of a path coefficient using the t-test. Because PLS simultaneously estimates the measurement model and the relationships between constructs, the item weights of formative constructs demonstrate the importance of their impact on information security. These weights of formative constructs can be interpreted similarly to estimated beta coefficients from a multiple regression analysis. The weights and t-statistics for the formative indicators are presented in Appendix Table 3.

In our model, resulting negative indicator weights (INFO_SEC5, HUM3, CULT3, ORG2, and COM5,7,9) presents an interpretation conundrum. One of the clearest interpretation of such a phenomenon is that a suppression effect is involved (Cohen and Cohen 1983). To investigate why some indicators negatively influence the underlying construct in our model, we examined whether a suppression effect has occurred (Cenfetelli and Bassellier 2009). This occurs when one independent variable (suppressor) suppresses the true effect of another. Conger (1974) defined a suppressor as a variable that increases the regression coefficient between the dependent and the independent variable by its inclusion in a regression equation. When the suppression effect is not controlled for, the relationship between one dependent and independent variable would appear smaller or even of opposite sign. We found that a suppression effect does not apply. We therefore tested, if the statistically negative weights have a positive bivariate correlation with the formatively measured constructs. This was the case for all three indicators (CULT3 = 0.630, ORG2 = 0.442, and COM5 = 0.516). We have therefore decided to include these indicators for the remaining analysis, because contrary to what we observe from the indicator weight alone, the indicators CULT3, ORG2, and COM5 are important in an absolute sense. Indicators with a non-significant negative weight (INFO_SEC5, HUM3, COM7,9) were removed (Cenfetelli and Bassellier 2009).

The data was collected via self-reported survey, thus the potential for common method variance (CMV) should be addressed (Chang et al. 2010; Doty and Glick 1998; McElroy et al. 2007; Podsakoff and Organ 1986). We tried to minimize these effects ex ante in the following ways: first, a number of procedural remedies in designing and administering the questionnaire were used to reduce the likelihood of CMV. We implemented the online survey questionnaire in such way as to prevent participants from back-tracking to change their answers. Counterbalancing the order of questions in the questionnaire in relation to different constructs makes CMV less likely, as the participant cannot then easily combine related indicators to cognitively create the correlation needed to produce a CMV-biased pattern of responses (Murray et al. 2005). Therefore, the pages of the survey items were presented in a random manner to discourage participants from figuring out the relationship between the dependent and independent constructs that we were trying to establish. Second, the anonymous nature of the survey would also mitigate the probability that respondents provided answers they believe were expected or self-serving answers. These remedies can ex ante reduce the likelihood of the theory-in-use biases and consistency motive in participants' responses (Chang et al. 2010; Podsakoff et al. 2003). Ex post, to access the common method bias, this study employed Harman's single-factor test (Podsakoff et al. 2003). All of the variables are loaded into an exploratory factor analysis (EFA) and the unrotated factor solution is

examined. Common method bias may exist if: first, a single factor emerges from the unrotated factor solution, or second, one general factor accounts for the majority of the covariance in the variables (Podsakoff et al. 2003). Although neither occurred in this study: no single factor accounted for a majority of the covariance. We also performed the test that was performed by Pavlou et al. (2007). The correlation matrix was examined to determine whether any constructs in the model correlated highly (> 0.9). In our model, the correlation matrix does not indicate highly correlated factors (highest correlation was 0.466). While the results do not preclude the possibility of CMV, they do suggest that CMV is not of great concern and thus is unlikely to confound the interpretation of the results.

Discussion and recommendations

This paper shows that personality traits are influential in determining attitudes towards holistic information security management. Figure 1 provides the estimates of the path coefficients and a summary of the test results of research hypotheses. In addition to the main focus of our study, the results indicate a strong statistical significance ($p < 0.001$) of the attitude towards organizational dimension as main predictor of an information security executive's intention to apply information security in a holistic focus. Our findings further suggest that technical, strategic and compliance dimensions ($p < 0.01$) are positively related to intention. Interestingly, the attitude towards the human and the contextual connected dimension of culture does not significantly influence the intention construct (HUM: t-value 1.093; CULT: t-value 1.158). This could be because the fact that the human dimension is regarded differently due to the diversity of empirical data in the context of organization size and industry. It is possible that information security executives still do not emphasize the human dimension in the context of information security management.

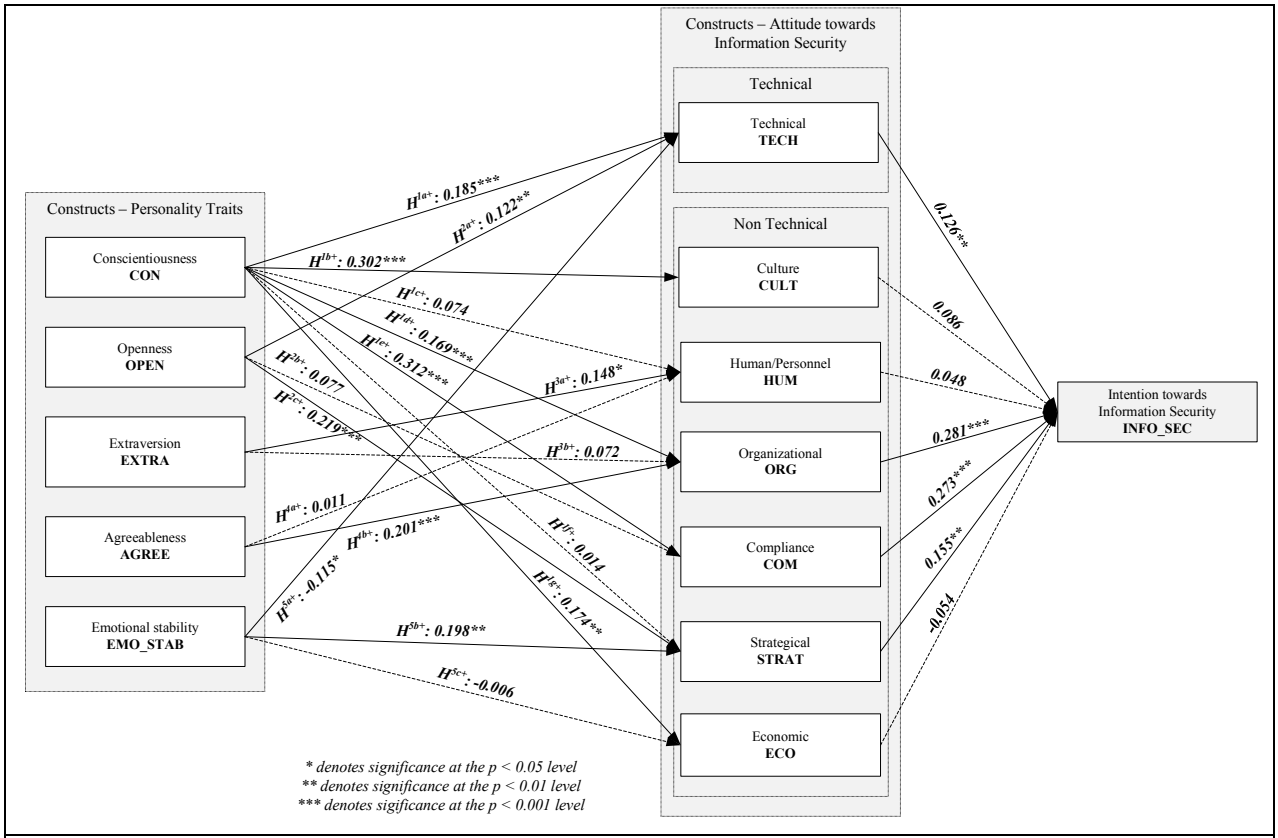

Figure 1. Structural model results

Further, the results of our study indicate that attitudes towards different information security management dimensions vary depending on different personality traits. More specifically, out of the

seven hypothesized relationships between conscientiousness and information security management, five significantly positive relationships were identified. However, because conscientiousness is a valid predictor in job performance (Barrick et al. 2001) our results are not surprising. Information security executives who score high in conscientiousness are persistent and more motivated towards goal-directed behavior, which can imply a more structured focus on the five dimensions of information security management. Even if the results are largely in support of our hypotheses, the human (H1c) and the strategic (H1f) dimensions of information security management were not found to be influenced by conscientiousness. However, prior research has shown that personality traits vary in their respective relevance (Barrick et al. 2001; Junglas et al. 2008). Upon reflection, a reason for not supporting H1c and H1f could be the specific topic of information security management. One reason for non-significance of H1c could be that information security executives' attitudes towards the human dimension of information security management are affected by both a positive information security culture and preventative technical measures being taken to protect information assets. Conscientiousness is shown to be positively related to both. Preventative technical measures, for example, can reduce the attitude towards the human dimension of information security management. Further, strategic information security management indicates more risky decision-making with high chances of failure. Even if conscientiousness is hypothesized to positively influence the attitude towards the strategic dimension of information security management, handling unforeseen issues or failures are no elements of conscientiousness facets.

Open information security executives react flexibly and critically examine changes in existing requirements, norms, and rules. Openness was hypothesized to have a positive relationship to the technical, strategic, and compliance dimensions of information security management. Information security executives who are open and receptive to new ideas, to experiencing new things, and who have broad life experience are more likely to form positive attitudes towards the technical and strategic dimension of information security management. A significant relationship between the openness and compliance (t-value 1.588) dimension of information security management cannot be identified, but the significance level is near $p = 0.10$. Upon reflection, it appears that information security executives who are creative and unconventional cannot act on these traits due to the need to comply with regulatory requirements. Strict regulatory requirements leave little room for flexibility.

Turning to extraversion, the path coefficient is significantly positive in relation to the human dimension of information security managenent ($\beta = 0.148$; $p < 0.05$); the influence of extraversion on the organizational dimension of information security management was not found to be influential (t-value 1.498). This highlights the importance of personality when considering interpersonal interactions, especially those associated with security training or awareness programs, in which interpersonal interaction is an essential factor for success (Da Veiga and Eloff 2007; Torres et al. 2006). Second, the results indicate that extraverted information security executives emphasize communication with end-user, for example. These findings are in accordance with Whitten (2008), who saw the need for strong soft skills in information security management. Mount et al. (2005) stated that the motive to interact with others is indicated by social interests from inside an individual, but it also refers to real social interaction from outside. It can be argued that extraverted information security executives form deeper positive attitudes towards the human dimension than they do toward the organizational dimension of information security management, because in the human dimension, there is more interpersonal interaction from outside. Extraversion fails to show a significant influence on the organizational dimension.

Agreeable information security executives are hypothesized to show a positive relation to the human and organizational dimensions of information security management. In prior research, it was pointed out that in a situation that requires interpersonal interaction, agreeableness appears to show a high predictive validity. In terms of information security executives' responsibilities, such as vertically communicating to the top management level, a positive significant relationship is shown ($\beta = 0.180$; $p < 0.001$). As pointed out by Whitten (2008), information security executives need good communication skills, and these are useful in the organizational dimension of information security management. Interestingly, no significant positive relationship to the human dimension could be identified. Due to its facets, agreeable individuals tend to trust their environment and strive for harmony in their social relationships (Junglas et al. 2008). Therefore, a reason for non-significance can be that information security executives' attitudes towards the human dimension of information security management are diversified. Because of a huge body of literature dealing with the human factor in information security management, information security executives might not share a common way of handling the challenge. Diverse implications could have led

to different opinions of the human information security management dimension. This may be one of the reasons why agreeableness did not significantly influence the human dimension.

Finally, as hypothesized, the results indicate that emotional stability has a positive impact on the strategic dimension of information security management, but a negative effect on the technical dimension; the impact on economical dimensions is not significant. Emotional stability is positively related to strategic dimension of information security management, with its challenges and requirements. Contrary to our expectations, emotional stability has a negative impact on the technical dimension of information security management. Prior research stated that emotionally stable individuals are likely to view innovative technical advances in their job as helpful and important (Devaraj et al. 2008). One explanation for the negative relationship we found between emotional stability and an information security executive's attitude towards the technical dimension could possibly be due to the sensitive environment. Emotional stability has been found to be negatively related to hazard factors (Chauvin et al. 2007). The experience in information security incidents might be overestimated by emotionally stable information security executives in a way that leads to worse attitudes towards preventative technical security measures. Therefore, emotionally stable information security executives are more likely to build negative attitudes towards the technical dimension of information security management. On the other hand, a divergent as expected relationship, as well as a lack of significance of the relationship between this personality trait and attitude is not surprising. As Junglas et al. (2008) explained in their research study, emotional stability shows its facets only in affective situations. This indicates that emotional stability is only significant in a trait-relevant situational cue (Junglas et al. 2008). Technical and economical information security management dimensions do not initiate affective cues.

Implications for research and practice

The findings have theoretical and practical implications. First, personality traits are an important issue in IS research and have been shown to be an important aspect in the specific context of information security management. Prior research has focused on tasks and skills of information security executives, and very few studies have focused on the behavioral patterns and how these elements impact the information security. This paper can be seen as a first step towards understanding the influence of personality traits on a holistic information security management approach. Knowing that personality traits are stable over time, short-term effects that mainly influence the cognitive processes of an information security executive in his or her daily tasks can be integrated into this model. For instance, the influence of others on an individual behavioral outcome as proposed by the subjective norm construct within the TPB can be integrated. Further, it would be interesting to determine whether there is empirical support for our propositions in an international context and if cultural and regulatory differences might affect the findings. Alternatively, rather than focusing on a holistic information security management approach, future research might focus on one specific dimension in detail and investigate the influence of selective personality traits. For example, due to its non-significance, agreeableness and the human dimension of information security management could be focused on in more detail. Together with other behavioral patterns, this research can open an area for the development of a comprehensive model for assessing holistic information security management in organizations or companies. Further research is also needed to explore whether external cues influence both personality traits and attitudes towards information security management. For instance, it is possible that the industry and organization size, and as a result, stricter regulatory requirements could affect attitudes towards specific dimensions of information security management.

From a practical perspective, the results indicate that there is no "one size fits all" approach. An information security executive's personality traits affect his or her attitude towards information security management dimensions, and it can be assumed that his or her focus would also be different. Even if regulatory requirements and other policies and standards guide information security executives in their daily tasks, their attitudes and behavioral patterns are different. Consequently, if a company understands the behavior traits of its information security executives, it can improve the information protection level. For example, these results might help organizations and companies in selecting team members in order to secure a specific part of their information or to enhance the effectiveness in an information security project. Analysis of personality traits, taken together with other human resources (HR) tools, can help HR and/or IS managers to find the right person for an information security position. Taking an organization's

strategic path in the protection of informational assets into account, management can staff the position in order to specifically improve the security level within the different dimensions. Furthermore, established management approaches can be extended, taking the individual differences of their information security executives into consideration. With the focus on a holistic information security management approach, this paper might also help develop or assess an executive's capabilities. Studying existing management teams that are responsible for information security, stronger regulation, supervision, and control procedures can enhance the protection level to ensure information security.

Limitations

The study is subject to following limitations. First, it is assumed that personality traits can be measured. The standardized and validated FFM personality traits used represent a generally accepted model in research. The FFM model measures individual differences in five dimensions. It cannot be precluded that unacknowledged factors are not considered. Culturally driven individual differences are not part of this personality model. A further limitation is that participants are from German-speaking countries. If we consider cultural and legal differences, it is likely that executives who are responsible for information security in other countries might have different attitudes about or reactions to the protection of informational assets. For example, Hofstede and McCrae (2004) found cross-national differences in personality traits. Future studies could expand to include an international context by integrating cultural differences and legal requirements into the evaluation of information security to identify potential security levels, taking individual differences into account. Caution must be taken when generalizing the findings to any industries. In order to show a general relationship between personality traits and attitudes towards holistic information security management, empirical data was collected with no special focus on industry or organizational size. Therefore, in order to increase generalizability follow-up studies are recommended to examine the effects of the size and type of organization. Further, we did not focus on a specific personality dimension, this could be examined in future with a specific focus on each personality dimension. Other opportunities for future research include the investigation of personality traits as potential moderators of the relationship between attitudes and intentions.

Conclusion

This paper served as an initial attempt to investigate the relationship between personality traits and holistic information security management. Recent studies have acknowledged the influence of personality on IS success outcome factors, however, incorporating personality traits from executives' perspective into information security management dimensions has largely been ignored. Personality was measured by the FFM; holistic information security management was measured by the attitude towards technical and non-technical dimensions of information security management – the latter represented by six components: strategy, organization, human, culture, compliance and economy. Results indicate that personality traits are influential in the context of information security management. For example, out of the FFM, conscientiousness, and agreeableness were found to positively influence an information security executives' attitude towards organizational information security management component. In addition, emotional stability and openness were found to significantly influence the attitude towards strategic information security management component.

Acknowledgements

The authors would like to thank the associate editor and the anonymous reviewers for their constructive, helpful feedback. One of the reviewers also provided very interesting ideas for future research. The authors also thank Dr. Robert Pomes and Dr. Claudia M. König, Hannover, for their valuable ideas and comments on their research in the early stages.

Appendix

Table 4. Formative constructs – Information security components			
Sources	Measurement item (translated from German)	Weight	t-stat
Intention towards information security (new items)	INFO_SEC1 : I intend to focus information security in a holistic manner	0.482	5.834***
	INFO_SEC2 : I intend to support technical and non-technical issues of information security in my organization	0.361	4.024***
	INFO_SEC3 : I intend to receive information about current global security issues within the next 30 days	0.527	6.130***
	INFO_SEC4 : I predict that I will check for lack of integrity, availability and confidentiality within the next 3 months	0.489	6.833***
	INFO_SEC5 : I plan to check for shortcommings within technical and non-technical information security environment	removed	
	INFO_SEC6 : I intend to carry out my responsibilities in consideration of technical and non-technical security issues	0.107	1.831°
Culture (Da Veiga and Eloff 2007; Werlinger et al. 2008)	CULT1 : I like the challenge to incorporate information security into the everyday practices of an employee's job	0.704	6.556***
	CULT2 : I feel responsible for communicating the right information security culture	0.531	4.282***
	CULT3 : Enforcing ethical conduct, for example not using the internet for private purpose during work, makes my work more interesting	-0.335	2.851**
	CULT4 : From my point of view, lack of security culture makes it difficult to change employees' existing security practices	0.301	2.439*
Organizational (Saleh et al. 2007; Ma and Pearson 2005; Park et al. 2010; ISO 27002)	ORG1 : I think security breaches should be reported as quickly as possible to top management level	0.361	3.782***
	ORG2 : The use of an information security forum to give management direction and support is a useful tool in my work	-0.265	3.499***
	ORG3 : The processing and management of third party agreements that cover relevant security requirements makes my work interesting	0.612	8.943***
	ORG4 : Ensuring that information security goals are identified and meet the organizational requirements are essential in my organization	0.222	2.233*
	ORG5 : The management of access rights in a distributed and networked environment enriches my daily work	0.510	6.157***
Human (Werlinger et al. 2008; Saleh et al. 2007)	HUM1 : I like to inform end-users about current security issues	0.694	3.982***
	HUM2 : Awareness trainings or other educational trainings make my work interestingly	0.719	4.426***
	HUM3 : From my point of view, information security behavior needs to be directed and monitored to ensure compliance	removed	
Technical (Anderson and Agarwal 2010; Johnston and Warketin 2010; ISO 27002)	TECH1 : Security measures such as implementing anti-virus software, firewalls, or backup systems are important in my organization	0.555	6.124***
	TECH2 : Technical security measures make work more interesting	0.326	3.099**
	TECH3 : Working with backup and recovery systems is enjoyable	0.379	3.837***
	TECH4 From my point of view, physical barriers are a useful tool to prevent unauthorized physical access and environmental contamination	0.214	2.069*
Economic (Park et al. 2010; ISO	ECO1 : I enjoy the challenge to manage information security cost effectively	0.113	0.353
	ECO2 : In my view, financial resources have always been one of	0.960	5.168***

27002)	the critical success factors in implementing information security		
Strategic (ISO 27001; ISO 27002)	STRAT1 : A business continuity management process is useful to minimize the impact on the organization and recover from loss of information assets	0.498	2.489*°
	STRAT2 : The goals and principles of information security in my organization should be in line with the business strategy and objectives	0.159	0.791
	STRAT3 : I enjoy paying attention to the information security strategy in order to protect information	0.830	5.914***
Compliance (Saleh et al. 2007; Ma and Pearson 2005; Da Veiga and Eloff 2007; ISO 27002)	COM1 : Security roles and responsibilities of employees should be documented in the security policy	0.149	2.183*
	COM2 : Contractual security obligations should be agreed and signed by employees	0.278	2.858**
	COM3 : Routinely reviewing audit logs is important in my organization	0.234	2.927**
	COM4 : In my opinion updating security policies is essential to establish a secure environment	0.493	6.505***
	COM5 : Information security policies should have a clear owner who is responsible for its update and maintenance	-0.200	2.341*
	COM6 : The design of protection and guidelines for working in secure areas makes my work enjoyable	0.122	1.192
	COM7 : I like the idea of regular checks of IS for compliance with security implementation standards	removed	
	COM8 : I enjoy the work with information security controls and their adequate application	0.137	2.034*
	COM9 : From my point of view, a security policy should define and authorize the consequences of violation	removed	
	COM10: I enjoy the challenge of working with regulatory and legal requirements	0.144	1.346
	COM11 : I think information security standards for example ISO / IEC 27002 enhance my daily work processes	0.173	2.165*
	COM12 : I like the use of formal mechanism such as policies, procedures and processes to enforce information security compliance	0.327	4.400***

References

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A multimethod empirical examination of home computer user behavioral intentions," *MIS Quarterly* (34:3), pp. 613-643.

Ashenden, D. 2008. "Information security management: A human challenge?" *Information Security Technical Report* (13:4), pp. 195-201.

Bagozzi, R. P. 2011. "Measurement and meaning in information systems and organizational research: Methodological and philosophical foundations," *MIS Quarterly* (35:2), pp. 261-292.

Bansal, G. 2011. "Security concerns in the nomological network of trust and Big5: First Order Vs. Second Order," in: *Proceedings of the 32nd International Conference on Information Systems*, Shanghai (China), Paper 9.

Barrick, M. R., Mount, M. K., and Judge, T. A. 2001. "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* (9:1/2), pp. 9-29.

Bedingfield, J. D., and Thal, A. E. 2008. "Project manager personality as a factor for success," in: *Proceedings of Portland International Center for Management of Engineering and Technology*, Cape Town (South Africa), pp. 1303-1314.

Benlian, A., and Hess, T. 2010. "Does personality matter in the evaluation of ERP Systems? Findings from a conjoint study," in: *Proceedings of the 18th European Conference on Information Systems*, Pretoria (South Africa), Paper 109.

Bhattacherjee, A., and Premkumar, G. 2004. "Understanding changes in belief and attitude toward information technology usage: A theoretical model and longitudinal test," *MIS Quarterly* (28:2), pp. 229-254.

Bulgurcu, B., Cavusoglu, Ha., and Benbasat, I. 2010. "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* (34:3), pp. 523-548.

Cavusoglu, Hu., Mishra, B., and Raghunathan, S. 2005. "The value of intrusion detection systems in information technology security architecture," *Information Systems Research* (16:1), pp. 28-46.

Chang, S.-J., van Witteloostuijn, A., and Eden L. 2010. "From the Editors: Common method variance in international business research," *Journal of International Business Studies* (41), pp. 178-184.

Chin, W. W. 1998. "Issues and opinion on structural equation modeling," *MIS Quarterly* (29:3), pp. vii-xvi.

Cohen, A. J., and Cohen, P. 1983. Applied Multiple Regression/Correlation Analysis for Behavioral Sciences, Hillsdale, NJ: Lawrence Erlbaum Associates.

Conger, A. J. 1974. "A Revised Definition for Suppressor Variables: A Guide to Their Identification and Interpretation," *Educational and Psychological Measurement* (34:1), pp. 35-46.

Costa, P. T. Jr., and McCrae, R. R. 1992. Revised NEO Personality Inventory (NEO-PI-R) and NEO Five Factor Inventory (NEO-FFI) professional manual, Odessa, Fl: Psychological Assessment Resources.

Costa, P. T. Jr., McCrae, R. R., and Dye, D. 1991. "Facet scales for agreeableness and conscientiousness: A revision of the NEO Personality Inventory," *Personality Individual Differences* (9:12), pp. 887-898.

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

Da Veiga, A., and Eloff, J. H. P. 2007. "An information security governance framework," *Information Systems Management* (24:4), pp. 361-372.

Devaraj, S., Easley, R. F., and Crant, J. M. 2008. "How does personalty matter? Relating the Five-Factor Model to Technology Acceptance and Use," *Information Systems Research* (19:1), pp. 93-115.

Diamantopoulos, A. 2011. "Incorporating formative measures into covariance-based structural equation models," *MIS Quarterly* (35:2), pp. 335-358.

Diamantopolous, A., Riefler, P., and Roth, K. P. 2008. "Advancing formative measurement models," *Journal of Business Research* (61:12), pp. 1203-1218.

Diamantopolous, A. and Siguaw, J. A. 2006. "Formative versus reflective indicators in organizational measure development: a comparison and empirical illustration," *British Journal of Management* (17:4), pp. 263-282.

Doty, D. H., and Glick, W. H. 1998. "Common methods bias: Does common methods variance really bias results?," *Organizational Research Methods* (1:4), pp. 374-406.

Eloff, J. H. P., and Eloff M.M. 2005. "Information security architecture," *Computer Fraud & Security* 2005 (11:1), pp. 10-16.

Fishbein, M., and Aijzen, I. 1975. Beliefs, Attitude, Intention and Behaviour: An Introduction to Theory and Research, Reading, MA: Addison-Wesley.

Fornell, C., and Bookstein, F. L. 1982. "Two structural equation models: LISREL and PLS applied to Consumer Exit-Voice Theory," *Journal of Marketing Research* (19), pp. 440-452.

Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables

and Measurement Error," Journal of Marketing Research (18), pp. 39-50.

Goswami, S., Teo, H. H., and Chan, H. C. 2009. "Decision-maker mindfulness in IT adoption: The role of informed culture and individual personality," in: *Proceedings of the 30th International Conference on Information Systems*, Phoenix (USA), Paper 203.

Haenlein, M., and Kaplan, A. M. 2004. "A Beginner`s Guide to Partial Least Squares Analysis," *Understanding Statistics* (3:4), pp. 283-297.

Hofstede, G., and McCrae, R. R. 2004. "Personality and culture revisited: Linking traits and dimensions of culture," *Cross-Cultural Research* (38:1), pp. 52-88.

Holland, J. L., Johnston, J. A., Asama, N. F., and Polys, S. M. 1993. "Validating and using the careers beliefs inventory," *Journal of Career Development* (19:1), pp. 233-244.

Hough, L. M. 1992. "The Big Five personality variables – construct confusion: Description versus prediction," *Human Performance* (5:1), pp. 139-155.

Howell, J. M., and Avolio, B. J. 1993. "Transformational Leadership, Transactional Leadership, Locus for Control, and Support for Information: Key Predictors of Consolidated-Business-Unit Performance," *Journal of Applied Psychology* (78:6), pp. 891-902.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2008. "Top Management Championship and Individual Behavior Towards Information Security: An Integrative Model," in: *Proceedings of the 16th European Conference on Information Systems*, Galway (Ireland), pp. 1310-1321.

Hu, Q., Hart, P., and Cooke, D. 2006. "The role of external influence on organizational information security practices: An institutional perspective," in: *Proceedings of the 39th Hawaii International Conference on Systems Sciences*, Kauai (USA), pp. 1-10.

International Organization for Standardization and International Electrotechnical Commissions. 2005. "ISO/IEC 27001:2005: Information Technology – Security Techniques – Information Security Management Systems – Requirements."

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

Judge, T. A., and Ilies, R. 2002. "Relationship of personality to performance motivation: A meta-analytic review," *Journal of Applied Psychology* (87:4), pp. 797-807.

Junglas, I. A., Johnson, N. A., and Spitzmüller, C. 2008. "Personality Traits and Concern of Privacy: An empirical Study in the Context of Location-Based Services," *European Journal of Information Systems* (17:4), pp. 387-402.

Karahanna, E., and Watson, R. T. 2006. "Information systems leadership," *IEEE Transactions on Engineering Management* (53:2), pp. 171-176.

Kotulic, A. G., and Clark, J. G. 2004. "Why there aren't more information security research studies," *Information & Management* (41:5), pp. 597-607.

Krankanhalli, A, Hock-Hai, T, Bernard, C. Y. T., and Kwok-Kee W. 2003. "An integrative study of information systems security effectiveness," *International Journal of Information Management* (23:2), pp. 139-154.

Krishnan, S., Lim, V.K.G., and Teo, T.S.H. 2010. "How does personality matter? Investigating the impact of Big-Five personality traits on cyberloafing," in: *Proceedings of the 31st International Conference on Information Systems*, Saint Louis (MO, USA), paper 6.

Kritzinger, E., and Smith, E. 2008. "Information security management: An information security retrieval and awareness model for industry," *Computer and Security* (27:5-6), pp. 224-231.

Lauriola, M., and Levin, I. P. 2001. "Personality traits and risky decision-making in a controlled experimental task: An exploratory study," *Personality and Individual Differences* (31:2), pp. 215-226.

Lee, Y., and Larsen, K. R. 2009. "Threat or coping appraisal: determinants of SMB executives' decision to

adopt anti-malware software," *European Journal of Information Systems* (18:2), pp. 177-187.

Li, Y., Chan-Ho, T., Hock-Hai, T., and Tan, B. 2006. "Innovative usage of Information Technology in Singapore organizations: Do CIO characteristics make a difference?" *IEEE Transactions on Engineering Management* (53:2), pp. 177-190.

Ma, Q., and Pearson. J. M. 2005. "ISO 17799: Best practices in information security management?" *Communications of the Association for Information Systems* (15:1), pp. 577-591.

MacCallum, C., and Browne, M. W. 1993. "The use of causal indicators in covariance structure models: Some practical issues," *Psychological Bulletin* (114:3), pp. 533-541.

MacKenzie, S. B., Podsakoff, P. M., and Podsackoff, N. P. 2011. "Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques," *MIS Quarterly* (35:2), pp. 293-334.

May, J., and Dhillon, G. 2010. "A holistic approach for enriching information security analysis and security policy formation," in: *Proceedings of the 18th European Conference on Information Systems*, Pretoria (South Africa), Paper 146.

McCrae, R. R., and Costa, P. 1999. "A five factor theory of personality," in: *Handbook of personality – Theory and research*, L. A. Lawrence and O. P. John (eds.), New York: Guilford Press, pp. 139-153.

McCrae, R. R., and John, O. P. 1992. "An introduction to the Five-Factor Model and its applications," *Journal of Personality* (60:2), pp. 175-215.

McElroy, J. C., Hendrickson, A. R., Townsend, A. M., and DeMarie, S. M. 2007. "Dispositional factors in internet use: Personality versus cognitive styles," *MIS Quarterly* (31:4), pp. 809-820.

Mount, M. K., Barrick, M. R., and Stewart, G. L. 1998. "Five-Factor model of personality and performance in jobs involving interpersonal interactions," *Human Performance* (11:2-3), pp. 145-165.

Mount, M. K., Barrick, M. R., Scullen, S. M., and Rounds, J. 2005. "Higher-order dimensions of the big five personality traits and the big six vocational interest types," *Personnel Psychology* (58:2), pp. 447-478.

Murray, J. Y., Kotabe, M., and Zhou, J. N. 2005. "Strategic alliance-based sourcing and market performance: Evidence from foreign firms operating in China," *Journal of International Business Studies* (36:2), pp. 187-208.

Nov, O., and Ye, C. 2008. "Personality and Technology Acceptance: Personal innovativeness in IT, openness and resistance to change," in: *Proceedings of the 41st Hawaii International Conference on System Science*, Big Island (Hawaii, USA), Paper 448.

Nunnally, J. C. (1978). *Psychometric Theory*. New York: McGraw-Hill.

Park, S., Ahmad, A., and Ruighaver, A. B. 2010. "Factors influencing the implementation of information systems security strategies in organizations," in: *Proceedings of the 2nd International Conference on Information Science and Applications*, Seoul (South-Korea), pp. 1-6.

Pavlou, P. A., Liang, H. and Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), pp. 105-136.

Petter, S., Straub, D., and Rai, A. 2007. "Specifying formative constructs in information systems research," *MIS Quarterly* (31:4), pp. 623-656.

Pierce, E. A., and Hansen, S. W. 2008. "Leadership, Trust, and Effectiveness in Virtual Teams," in: *Proceedings of the 29th International Conference on Information Systems*, Paris (France), Paper 43.

Podsakoff, P. M., Organ, D. 1986. "Self-Reports in Organizational Research: Problems and Prospects," *Journal of Management* (12:4), pp. 531-544.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.

Renner, W. 2002. "A psychometric analysis of the NEO Five-Factor Inventory in an Austrian Sample," *Review of Psychology* (9:1), pp. 25-31.

Ruighaver, A. B., Maynard, S. B., and Chang, S. 2007. "Organisational security culture: Extending the end-user perspective," *Computer & Security* (26:1), pp. 56-62.

Saleh, M. S., Alrabiah, A., and Bakry, S. H. 2007. "Using ISO 17799:2005 information security management: a STOPE view with six sigma approach," *International Journal of Network Management* (17), pp. 85-97.

Sharma, R., and Yetton, P. 2003. "The contingent effects of management support and task interdependence on successful information systems implementation," *MIS Quarterly* (27:4), pp. 553-556.

Shropshire, J., Warkentin, M., Johnston, A. C., and Schmidt, M. B. 2006. "Personality and IT security: An application of the five-factor model," in: *Proceedings of the 12th Americas Conference on Information Systems*, Acapulco (Mexico), pp. 3443-3449.

Siponen, M., and Willison, R. 2009. "Information security management standards: Problems and solutions," *Information & Management* (46:5), pp. 267-270.

Smaltz, D. H., Sambamurthy, V., and Agarwal, R. 2006. "The antecedents of CIO effectiveness in organizations: An empirical study in the healthcare sector," *IEEE Transactions on Engineering Management* (53:2), pp. 207-222.

Spector, P. E., Jex, S. M., and Chen, P. Y. 1995. "Relations of incumbent affect-related personality traits with incumbent and objective measures of characteristics of jobs," *Journal of Organizational Behavior* (16:1), pp. 59-65.

Stanton, J. M., Stan, K. R., Mastrangelo, P., and Jolton, J. 2005. "Analysis of end user security behaviors," *Computer & Security* (24:2), pp. 124-133.

Straub, D. W., and Welke, R. J. 1998. "Coping with systems risk: security planning models for management decision making," *MIS Quarterly* (22:4), pp. 441-469.

Streiner, D. L. 2003. "Starting at the Beginning: An Introduction to Coefficient Alpha and Internal Consistency," *Journal of Personality Assessment* (80:1), pp. 99-103.

Sun, H. 2012. "Understanding User Revisions when Using Information System Features: Adaptive System Use and Triggers," MIS Quarterly (36:2), pp. 453-478.

Taylor, R. 2006. "Management perception of unintentional information security risks," in: *Proceedings of the 27th International Conference on Information Systems*, Milwaukee (USA), pp. 1581-1597.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2005. "The insider threat to information systems and the effectiveness of ISO 17799," *Computers & Security* (24:6), pp. 472-484.

Torres, J. M., Sarriegi, J. M., Santos, J., and Serrano, N. 2006. "Managing information systems security: Critical success factors and indicators to measure effectiveness," in: *Proceedings of the 9th International Conference on Information Security*, Samos Island (Greece), pp. 530-545.

Vroom, C., and von Volms, R. 2004. "Towards information security behavioural compliance," *Computers & Security* (23:3), pp. 191-198.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems* (20:1), pp. 267-284.

Werlinger, R., Hawkey, K., and Beznosov, K. 2008. "An integrated view of human, organizational, and technological challenges of IT security management," *Information Management & Computer Security* (17:1), pp. 4-19.

Wetzels, M., Odekerken-Schroder, G., and van Oppen, C. 2009. "Using PLS Path Modeling for Assessing Hierachical Construct Models: Guidlines and Empirical Illustration," *MIS Quarterly* (33:1), pp. 177-195.

Whitten, D. 2008. "The chief information security officer: An analysis of the skills required for success," *Journal of Computer Information Systems* (48:3), pp. 15-19.

Zafar, H., Clark, J. G. 2009. "Current state of information security research in IS," *Communications of the Association for Information Systems* (24), pp. 571-596.

Zhao, X., Xue, L., and Whinston, A. B. 2009. "Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling," in: *Proceedings of the 30th International Conference on Information Systems*, Phoenix (USA), Paper 49.