Computer and Information Science; Vol. 14, No. 1; 2021
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Personality and Employees' Information Security Behavior among Generational Cohorts

Cartmell Warrington[1], Javaid Syed[2], Ruth M. Tappin[3]

[1] Dept. of Computer Science and Technology, SUNY Orange, New York, United States

[2] Salem University, WV, United States

[3] R.M. Tappin, LLC, NH, United States

Correspondence: Cartmell Warrington, Dept. of Computer Science and Technology, Orange County Community College, (SUNY Orange), 115 South St, Middletown, NY 10940, United States.

This research was not financed or sponsored by any academic, corporate, or governmental agency or entity.

Received: December 14, 2020 Accepted: January 11, 2021 Online Published: January 22, 2021

doi:10.5539/cis.v14n1p26 URL: https://doi.org/10.5539/cis.v14n1p26

Abstract

The Big Five Factors Model (FFM) of personality traits theory was tested for its ability to explain employee information security behavior (EISB), when age, measured by generational cohort (GCOHORT), moderated the relationship between the independent variables (IVs) extraversion, agreeableness, conscientiousness, emotional stability, intellect (EACESI) and the dependent variable (DV), employees' information security behavior (EISB) which is measured by file protection behavior (FPB). Three age groups defined GCOHORT: 52–70 years old (1946–1964, Baby Boomers), 36–51 yrs old (1965–1980, Generation X), and 18– 35 yrs. Old (1981–1998, Millennial). Results of hierarchical multiple regressions analyses revealed statistically significant relationships between overall personality traits, four individual factors of personality traits, and the DV ($p < .05$). However, contrary to expectations, GCOHORT did not moderate the relationship between any of the main IVs and the DV ($p > .05$). Recommendations for future research are offered.

Keywords: big five factor model, cyber security, data breaches, data protection, generational age group, individual differences, information security behavior, InfoSec, personality traits

1. Introduction

In an era of big data, when organizations are now more reliant on information systems (InfoSys) for market gains and competitive advantage, data breaches are increasing with dizzying frequency. Goddijn (2019) reported the occurrence of 3813 data breaches by June 30th 2019, which exposed 4.1 billion of customers' records to cyber criminals; startlingly, this was a 54% increase in data breaches and a 52% increase in the number of exposed records compared to the same period in 2018. Emails and passwords accounted for 70% and 68% of breaches respectively. Although the publicly reported number of data breaches in the first Quarter of 2020 was 58% less than the same period in 2019, the likely reason for the decrease was partly due to reporting disruptions caused by COVID19 (Goddijn & Kouns, 2020).

Organizational insiders such as employees account for most data breaches, yet organizations allocate most of their resources to external and technical solutions to prevent these occurrences (Besnard & Arief, 2004; Choi et al., 2018). It is critical for organizational leaders to understand whether or how employees' personal differences inform their information security (InfoSec) or cybersecurity behaviors (Fatokun et al., 2019), and especially important to study personality traits in relation to InfoSec (Uffen, Guhr, & Breitner, 2012). However, there is a gap in the literature in understanding the relationship between employees' behaviors and data breaches since there is a paucity of research on the individual differences in this type of research (Gratian et al., 2017; Whitty et al., 2015). Repeatedly, calls have been made to study the phenomenon of data breaches and employee behaviors from a behavioral science perspective, and, in particular, with a focus on the correlation between personality traits and employees' information security (InfoSec) behaviors (e.g., Gratian et al., 2017; Lounsbury et al., 2014; Pattinson et al., 2015; Shropshire et al., 2015; Whitty et al., 2015;).

The problem that prompted this study is that there are conflicting reports about the relationship between various personality traits, age, and their correlation with employees' InfoSec behaviors (e.g., Gratian et al., 2017;

Haddington, 2018; McCormack et al., 2017; Nicholson et al., 2005; Pattinson et al., 2015). Therefore, the purpose of this research is to contribute to the sparse body of literature on personality traits and employees' InfoSec behaviors, based on employees' generational cohorts. Specifically, the InfoSec behavior under investigation is *file sharing behavior.*

2. Literature Review

For firms, as well as their customers, consequences of data breaches can be disastrous and can affect firm performance and customer confidence negatively (Martin et al., 2017; van Bavel et al., 2019). Organizations can suffer loss of investors' confidence, loss of market share and revenues, harm to the company's brand and reputation, loss of intellectual property, and decreased customer spending (Janakiraman et al., 2018). Consumers often suffer from firms' data breaches as well when their personally identifiable information become subject to identity theft, which can cause havoc in their personal and professional lives. Goddjin (2019) reported that approximately 70% of breaches were due to "unauthorized access to systems or services, while approximately 90% of the records exposed were attributable to exposing/publishing data online" (p. 2).

Traditional approaches to information security (InfoSec) management of data breaches have been rooted in technological solutions (Besnard & Arief, 2004; Choi et al., 2018). Despite major investments in external solutions for data protection, across industries the failure rate of InfoSec initiatives is extraordinarily high as businesses continue to bleed billions of dollars each year on various types of externally-focused initiatives, while overlooking insider human behavior (Choi et al., 2018; Leszczyna, 2013). However, there is now ample proof in the literature, which show that insiders' human errors and actions are responsible for as many as 33% to 90% of data breaches and cyber attacks (e.g., Budzak, 2016; Colwill, 2009; Shepherd & Kline, 2012; Shropshire et al., 2015; Zhen et al., 2020). According to Rafter (2020) in a report for Norton, a global company providing cyber security solutions to homeowners and businesses, employees are on the frontlines of InfoSec; however, they are the weakest links in InfoSec efforts (Gratian, et al., 2017; Vroom & von Solms, 2004). Employees indulge in risk-taking behavior that present a significant threat to InfoSec systems and controls when they exhibit poor information security behavior by not complying with the organization's policies and procedures (Ifinedo, 2014; Johansen, 2020; Kessler et al., 2019); however, consistently, employees overestimated the probability that they could fall victim to InfoSec breaches (Herath & Rao, 2009). Lahcen et al. (2020) postulated, "People's biases and behaviors influence the interactions with software and technology…" (p. 2). This had been borne out in the literature in earlier research (e.g. Shropshire et al., 2015; Vroom & von Solms, 2004).

Since firms collect copious amounts of sensitive industry and customer data, it behooves organizational leaders to protect this information; yet, incredibly, organizations focus most of their security control efforts on external solutions even though longstanding evidence has shown that the behaviors of organizational insiders account for most data breaches (Choi et al., 2019; Colwill, 2009; Jeong et al., 2019; Uffen, Guhr, & Breitner, 2012); indeed, employees' noncompliance with internal InfoSec measures as well as deliberate acts of revenge and sabotage account for most security breaches (Peikari & Banazdeh, 2019). Forms of employee noncompliance are rooted in human behaviors, which include seemingly benign acts such as treating information security measures lightly, to more egregious behaviors that can include committing deliberately malicious acts against the organization (Besnard & Arief, 2004; Colwill, 2009; Shepherd & Kline, 2012; Shropshire et al., 2015; Kessler et al., 2019).

In past studies related to technology acceptance and use, researchers tended to rely on theories such as the technology acceptance model (TAM) and the unified theory of acceptance and use of technology (UTAUT) to study employees' acceptance attitude toward IT and InfoSec. However, given the role that employees' behaviors play in data breaches, increasingly, researchers are turning to theories in the behavioral sciences for answers about how personality, cognition, and other behavior-related influences might inform employees' IS behavior (Pfleeger & Caputo, 2012; Uffen, Kaemmerer, & Breitner, 2013). In this study, a behavioral science approach is taken and the Big Five Factor Model (FFM) of personality traits provides the theoretical foundation for the research. The purpose of the study is to (a) investigate the efficacy of the FFM to predict employees' information security behavior (EISB), measured by file protection behavior (FPB), the dependent variable (DV), and (b) to understand the effect that generational age has on the relationship between the five individual factors of personality traits and FPB.

2.1 Behavioral Science Approach to Understanding IS Breaches

It is only in the last 15 – 20 years that interest emerged in applying a behavioral science approach to understanding the problem of InfoSec breaches. Studies on explanatory relationships between personality traits and InfoSec behaviors have been emerging as areas of interest in understanding human behavior in relation to information security; however, there is still a paucity of literature in this area of research (Gratian et al., 2017;

Shropshire et al., 2015); hence Shropshire et al. recommended continued InfoSec research grounded by behavioral theories. Nevertheless, despite the lack of a robust body of literature in this area, there are reports of correlations between personality trait variables and employees and consumers' behaviors toward information technology (IT) and information security behaviors (Cheng et al., 2013; Gratian et al., 2017; Patsiotis et al., 2013; Shropshire et al., 2015; Uffen, Kaemmerer, & Breitner, 2013).

2.2 Personality and Personality Traits

According to the American Psychological Association (2020), "personality refers to individual differences in characteristic patterns of thinking, feeling and behaving" and a trait is "a dynamic trend of behavior, which results from the integration of numerous specific habits of adjustment, and which expresses a characteristic mode of the individual's reaction to his surroundings" (Allport, 1927, p. 288). Personality traits are universal and inherent in all human beings across the globe, across all cultures, and influence human behaviors (Allik et al., 2017; Allport, 1927; Goldberg, 1993; McCrae & Costa, 1997) and has been reported to be stable and consistent over time (Costa et al., 2019; Damian, 2019; McCrae & Costa, 1997). However, Roberts and Mroczek (2008) cited several longitudinal studies, which show that personality traits are malleable, continue to change and develop during all phases of an individual's lifespan.

Because of its bearing on human behaviors, personality traits have been studied in a wide variety of organizational contexts for its relationship with human behavior and various organizational outcomes (Syed & Tappin, 2019). Due to the overwhelming evidence of the presence of five dominant personality traits under which other traits were clustered what became known as the "Five Factor Model" (FFM) of personality traits emerged. Barrick et al., (2003) posited, "The FFM model of personality describes the basic dimensions of personality at a global level" (p. 46). Eventually, this model of five dominant traits was dubbed the Big Five Factor Model (FFM).

2.2.1 The Big Five Factor Model of Personality Traits

Two FFMs popularly used in behavioral science research are the Revised NEO Personality Inventory (NEO-PI-R) model by Costa and McCrae (1992), which is referred to as the NEOAC model[1] and the Goldberg (1999) model, referred to by the acronym EACESI. The NEO PI-R derives from factor analyses of questionnaires and lower-order facets, and is arranged in a hierarchical order, as follows:

- Factor 1 = Neuroticism (*easily prone to emotional distress and stress; the opposite of* Emotional Stability);
- Factor 2 = Extraversion (*tendency toward risk-taking and intense and frequent interpersonal interactions*);
- Factor 3 = Openness to experience (*tendency to seek out new experiences*)
- Factor 4 = Agreeableness (*tendency to be helpful, sympathetic, unselfish*);
- Factor 5 = Conscientiousness (*tendency to be hardworking, detail and achievement oriented*).

The Goldberg (1999) model, used in this research, is not hierarchically ordered and is rooted in the lexical tradition; it is based on factor analyses of adjectives or descriptive words, as follows:

- Factor 1 = Extraversion/Surgency (*sociable* vs. *introverted*);
- Factor 2 = Agreeableness (*affable* vs. *reserved*);
- Factor 3 = Conscientiousness (*well-organized* vs. *wasteful*);
- Factor 4 = Emotional Stability vs. Neuroticism (*self-assured* vs. *insecure*);
- Factor 5 = Intellect/Imagination (*creative/resourceful* vs. *wary/guarded*).

It has long been established in the seminal and contemporary literature that, in social and organizational contexts, the FFM is suitable for studying human behaviors and dispositions. For example, risk-taking behavior is a characteristic of extraversion (Nicholson et al., 2005). In a study of participants in various organizational and social contexts, Nicholson et al. found positive relationships between high extraversion, agreeableness, and

[1] Note: Many research articles erroneously identify the NEO PI-R acronym for the Big Five as "OCEAN" and sometimes "CANOE". Since Costa and McCrae's Big Five model is based on a hierarchical order, the correct representation of the order should be NEOAC as described in Costa, McCrae, and Kay (1995) and earlier articles.

propensity for risk. According to Nicholson et al., low neuroticism and low conscientiousness insulate individuals against feelings of guilt or anxiety related to negative consequences of risk-taking. Furthermore, low conscientiousness "makes it easier to cross the cognitive barriers of need for control, deliberation and conformity" (p.170). Jackson et al., (2009) reported an increase in the conscientiousness trait with increased age. These findings have implications for employees' InfoSec behavior in regards to whether employees' personality traits explain or predict their file protection behaviors. In fact, in relation to InfoSec, it is important to study personality traits (Uffen, Guhr, & Breitner, 2012).

In the IT and InfoSec fields, the study of personality traits is emerging as an area where the behavioral sciences have been applied to investigate and explain employees' personality and InfoSec behaviors in relation to various organizational outcomes that range from organizational commitment to information security. For example, based on a national sample of IT professionals (N = 279), Syed and Tappin (2019) reported no statistically significant correlations between neuroticism and organizational commitment in a study of the relationship between the neuroticism factor of personality traits (IV), personal characteristics (IV) and organizational commitment (DV).

Specific to InfoSec, Uffen et al. (2012) reported conscientiousness was positively related to an individual's technical and organizational InfoSec activities. Pattinson et al. (2012) reported higher InfoSec behaviors against phishing emails among individuals who scored high on extraversion and openness (intellect); responding to phishing emails is risky InfoSec behavior as respondents are enticed to share sensitive information. Concerning the influence of individual differences on cognitive determinants of behavioral intention to use security measures among a sample of smartphone users (N = 435), Uffen, Kaemmerer, and Breitner (2013) reported that multiple facets of personality traits significantly affected cognitive determinants to predict intention to use security measures; for example, conscientiousness and extraversion were related positively to information security management, but openness was not positively related with intention to use security measures (Halevi, 2013; Uffen et al., 2013). Li et al. (2014), observing that individuals displayed similar online and offline behavior, confirmed behavioral consistency in file protection behavior among individuals online and in the workplace such that micro-blogging behavior predicted personality traits among a sample of Chinese micro bloggers (N = 547). Welk et al. (2015) found that individuals with lower scores on extraversion and anxiety were better at phishing detection; low anxiety is indicative of the emotional stability trait, while high anxiety is characteristic of neurotic individuals (Syed & Tappin, 2019). Jeske et al. (2016) confirmed some personality traits can predict human security behavior in smartphone use and on social media.

Shropshire et al. (2015) reported that, based on a sample of undergraduate college students (N = 170), attitudinal constructs confirmed evidence of behavior toward InfoSec measures, and two personality traits (conscientiousness and agreeableness) were positively related to intent to adopt IS measures. Pattinson et al. (2012), and Pattison et al. (2015) examined accidental-naïve (i.e., risky) behaviors such as inadvertently sharing passwords, opening attachments in unsolicited emails, which are types of InfoSec behaviors (Gratian et al., 2017; Hayden, 2009; Herath & Rao, 2009; Shropshire et al., 2015; Stewart & Jŭrgens, 2017; Whitty et al., 2015). Specifically, Pattinson et al. (2015) examined InfoSec related behaviors related to "password management, email use, Internet use, social networking site use, mobile computing, information handling, and incident reporting" (p. 5). Personality traits and age were among the variables examined by standard multiple regression analysis to explain InfoSec behavior. Findings were that individuals with low extraversion scores and high scores in agreeableness, conscientiousness, openness (intellect), as well as older individuals, were less likely to indulge in risky InfoSec behaviors; emotional stability was not statistically significantly related to InfoSec behavior.

McCormac et al. (2016) reported that agreeableness, conscientiousness, and emotional stability (the opposite of neuroticism) explained statistically significant variances in individuals' information security awareness (ISA). Russell et al., (2017) reported an inverse correlation between neuroticism and secure cyber behaviors such that as neuroticism increased, cybersecurity behaviors decreased. Neuroticism has been long associated with anxiousness, stress, and keener beliefs about impending threats, so the results by Russell et al. that neurotic individuals were less likely to practice secure cyber behavior was surprising. Russell et al. surmised that the high levels of worry and stress among neurotics might limit the mental resources required to maintain secure cyber behaviors. In a study of correlations between human personality traits (i.e., individual differences) and cybersecurity behavior intentions based on a sample of 369 students, faculty, and staff at a large public university, Gratian et al., 2017) reported, "individual differences accounted for 5%–23% of the variance in cyber security behavior intentions, and extraversion and gender were predictors of good security behavior" (p. 345).

A close examination of the InfoSec and personality traits literature revealed some conflicting results. Since this area of research is still developing, there is a need for further inquiries into whether behavioral sciences theories—and personality traits in particular—can explain employee IS behaviors (Shropshire et al., 2015).

Inspired by Shropshire, Johnson, Warkentin and Schmidt (2006) and Shropshire et al. (2015), we drew on literature on behaviors in organizational and social contexts as well as individuals' behaviors toward InfoSec adoption and use in a variety of contexts. In this study, we examine the effect that generational age exerts on the relationship between the FFM and employees' information security behavior to explain employees' file protection behavior.

2.3 Information Security (InfoSec)

The terms "information security" and "cybersecurity" have been used interchangeably in the literature (von Solms & van Niekerk, 2013), and is similarly applied in the present study. However, although the two terms carry analogous overlapping meanings related to the protection of data, von Solms and van Niekerk postulated that there are subtle differences in that cyber security goes further than InfoSec in that it includes human security in addition to data security. Wilner (2018) opined that "information security" is a more accurate and appropriate term than "cybersecurity" to describe protection of data. It is critical for organizations to understand how employees' personal differences inform their InfoSec (cybersecurity) behaviors (Fatokun et al., 2019) as there is a paucity of research on the individual differences in this type of research (Gratian et al., 2017; Whitty et al., 2015). For the purposes of this study, InfoSec is defined as the management and protection of an individual's or a company's information data and/or data assets (e.g. Cheng et al., 2013; Thompson & von Solms, 2005), and carries the same meaning as cybersecurity.

2.3.1 Employee Information Security Behaviors (EISB)

Employees' information security behavior (EISB) is the "core set of information security activities that have to be adhered to by end users to maintain information security as defined by information security policies" (Padayachee, 2012, p. 673). InfoSec behaviors include actions by individuals related to "running and updating security software, keeping passwords secure, running a firewall, enabling encryption for home wireless network, etc." (Villafranca, 2015, p. 159). In this study, the employee InfoSec behavior of interest is employees' attitude toward protecting their electronic files, or file protection behavior (FPB).

2.3.2 File Protection Behavior (FPB)

The dependent variable (DV), File protection behavior (FPB), is defined as limiting or allowing access to files on one's computer (Hayden, 2009; Shropshire et al., 2015). File protection behavior operationally defines employee information security behaviors (EISB). Activities related to FPB include—but are not limited to—following prescribed conventions regarding, for example, creating complex passwords; protecting passwords; sharing passwords; backing up data; data sharing; adhering to email policies; scanning documents, detecting; proactive awareness such as avoiding phishing emails; updating to keep abreast of security patches; device securement, and protecting access to sensitive electronic files (Gratian et al, 2017; Hayden, 2009; Herath & Rao, 2009; Shropshire et al., 2015; Stewart & Jŭrgens, 2017; Whitty et al., 2015). Despite emerging interest in investigating the problem of InfoSec through different theoretical lenses, to date, little is known about how behavioral science theories such as the FFM might explain information security behaviors among employees of different generational age groups as evidenced, for example, by their attitudes and behaviors concerning protection of their electronic files.

2.4 Age

Personal characteristics such as age, ethnicity, gender, geographic region, educational and socio-economic status, are common and important demographic variables used in social science research. Older individuals were shown to be generally more cautious and less prone to risk-taking (Nicholson et al., 2005). However, regarding InfoSec, age has been associated with risky behaviors (e.g., Chakraborty, Vishik, & Rao, 2013; Grimes, Hough, Mazur, & Signorella, 2010; McGhee, Ehrler, Buckhalt, and Phillips, 2012). Results of a study by Whitty et al. (2015) on the effects of age on password-sharing, which is one type of file-protection behavior, indicated that older people were more likely to share passwords. Contrarily, McCormac et al. (2016) found that age made no statistically significant contribution to information security awareness, and Gratian et al. (2017) found that the age demographic exerted no statistically significant unique effect on security behavior intention. However, more recently, Fatokun et al. (2019) reported a statistically significant relationship between age and cybersecurity behavior among two groups of younger (< 30 years old) and older (> 30 years old) college students, and Shappie, Dawson, and Debb (2019) reported age to be a significant predictor of cybersecurity behaviors.

Due to the widely accepted view concerning the stability of personality traits from childhood through adulthood, these findings carry implications concerning a variety of behaviors in adulthood, including security related behaviors. The seemingly conflicting reports regarding age and InfoSec behavior warranted further studies on

the phenomenon. For this study, age is measured by belongingness to one of three generational cohorts (GCOHORT) born between 1946–1964, 1965–1980, and 1981–1998.

2.4.1 Generational Cohort

According to reports from the Bureau of Labor Statistics (BLS), individuals enter the workforce earlier than age 18 and remain in it past the age of 70 (Toossi & Torpey, 2017). Generational cohorts are people with identical birth years, history, and share common or distinct experiences (Zemke, Raines, & Filipczak, 2000). Although the span of years is not typically absolute, the range of years for the generational cohorts falls between 15 to 20 years. The generational groups under investigation in the present study spanned the following periods: 1946–1964 (Baby Boomers); 1965–1980 (Generation X), and 1981-1998 (Millennial or Generation Y).

The cultural events, (historical, political, and social), as perceived by the generational cohorts, characterizes and influences their values, work ethics, attitude toward authority, and professional aspirations (Duchscher & Cowin, 2004). Different generations generally respond differently to phenomena in their environment, and these responses can inform organizational functioning in the workplace (Scroxton, 2020). For example, Villafranca (2015) reported Millennials showed a propensity to exhibit responsible InfoSec behaviors in relation to phishing and spamming, but lower awareness in regards to malware, viruses, worms, and Trojans; however, they become more security aware as they age. In a publication by the Society for Human Resource Management (SHRM), Hardy (2016) highlighted security concerns around Millennials' use of personal devices in the workplace and their perceptions about file sharing and use of social media at work. Garba, Armarego and Murray (2015) reported Generation X was more dependent on the use of their own devices at work, and the use of personal devices at work was fraught with InfoSec risks. Baby Boomers are perceived to be slow adopters of technology and not as cognizant of cyber threats as younger generations (Chakraborty et al., 2013; Grimes et al., 2010). This perception might create preconceived notions regarding InfoSec behavior in the workplace toward this generation, especially since Baby Boomers are using some types of social media at higher rates than succeeding generations (Clement, 2020; Madden, 2010). Sixty-eight percent of Baby Boomers use Face Book, and 70% of this generation uses YouTube actively (Clement, 2020). Since employees of all ages use social media at work and since these media have been identified with employee-related InfoSec behaviors (e.g., Ornstein & Huseman, 2015), it is important to study the behaviors of different generational cohorts to understand differences in their behaviors with regards to InfoSec.

Whitty et al. (2015) found that older individuals who scored high on self-monitoring, which is associated with conscientiousness, were more likely to share their passwords, hinting at a surprising lack of security awareness. Conscientiousness in individuals is known for attention to detail and high work ethics; perhaps older individuals with high expressions of this trait might actually be less cautious about their file protection behavior due to over confidence in their ability to be detail oriented. McCormac et al. (2016) reported that age did not statistically significantly explain any variance in InfoSec awareness such as attitude and behavior toward sharing password. The apparent conflicting results in the literature, the paucity of literature on the subject, and the knowledge gap in the InfoSec field presented the opportunity to investigate the problem further.

The stability of personality traits from youth through maturity has long been established in the literature; however, within the last decade research revealed changes in personality traits in adulthood, based on individual differences (Roberts & Mroczek, 2008). Therefore, it is reasonable to expect that generational age would affect the relationship between personality traits and employees' information security behavior (EISB). We were prompted to ask whether (a) the FFM had the power to explain a relationship between extraversion, agreeableness, conscientiousness, emotional stability, intellect (EACESI) and employees' InfoSec behavior (EISB), as measured by their file protection behavior (FPB), and whether generational age moderated the relationship between each of the five individual Big Five traits and FPB. The FFM is measured by the IVs, extraversion, agreeableness, conscientiousness, emotional stability, and intellect (Goldberg, 1999). Based on the conflicting evidence, paucity of literature, and gap in the literature, we propose the following hypotheses:

2.5 Hypotheses

H_1: Generational age will moderate the relationship between overall personality traits and employee's file protection behavior.

H_2: Generational age will moderate the relationship between extraversion and employee's file protection behavior.

H_3: Generational age will moderate the relationship between agreeableness and employee's file protection behavior.

H_4: Generational age will moderate the relationship between conscientiousness and employee's file protection behavior.

H_5: Generational age will moderate the relationship between emotional stability and employee's file protection behavior.

H_6: Generational age will moderate the relationship between intellect and employee's file protection behavior.

Null hypotheses (H_0) were that generational age will not moderate the relationship between all of the main IVs and the DV.

3. Method

In the study, overall personality traits, extraversion, agreeableness, conscientiousness, emotional stability, and intellect (EACESI) are the main independent variables (IVs), generational age cohort (GCOHORT), a second set of IVs, is the moderating variable (MV), and EISB is the dependent variable (DV). A multiple regressions model was appropriately applied to study relationships between the variables (Tabachnick & Fidell, 2007).

Employees' generational age is measured by 18 – 35 yrs old (Generation Y/Millennial, 1981 – 1998); 36 – 51 yrs old (Generation X, 1965 – 1980), and 52 – 70 yrs old (Baby Boomers, 1946 – 1964). The employees' information security behavior (EISB) construct is measured by the DV, file protection behavior (FPB), as evidenced by employees' attitude toward protecting their electronic files. To investigate relationships among the variables, the study drew upon a broad spectrum of computer users (N = 152) from diverse organizations within the United States (U.S.). These employees were all employed at the time the survey was taken, and all had access to sensitive files in their organization.

3.1 Overview

Analysis was at the employee level and a sample frame of employees who had access to sensitive electronic data in their organization was targeted from the population. Based on a G*Power 3.1.9.4 *a priori* calculation (Faul, Erdfelder, Buchner, & Lang, 2009), the sample size was 153 employees, which had the power (1-β err prob = 0.95) to detect a statistically significant (p = 0.05) medium-sized effect (f^2 = 0.15) in the sample. Qualtrics^{XM} returned responses from158 individuals with fully completed questionnaire surveys.

Six assumptions related to the multiple regressions model were checked to make a preliminary determination of the fitness of the data to use in the regression analysis; these assumptions are independence of errors, linearity, homoscedasticity, multicollinearity, significant outliers/influential points, and normality of distribution (Rahman, Sathik, & Kannan, 2012). Subsequently, of the 158 responses, six outliers were eliminated due to their influence of extreme skewness on the distribution of the data. All future analyses were based on the final sample size of n = 152.

Although some skewness of the data was still evident after removal of the outliers, the residuals were approximately aligned with the end points of the regression line. Regression analysis is robust to the distribution of data assumption (Osborne & Waters, 2002); therefore, the regression model was deemed appropriate for data analysis and, based on the ANOVA output ($p < .05$), the data were a good fit for the model.

3.2 Participants

The population of interest adults was employed within the U.S. at the time of data collection. Primary data collected by Qualtrics^{XM} were used in the study. Qualtrics^{XM} used random sampling probability techniques to select study participants from its panel of voluntary survey participants. The company followed established protocols for ethical research involving human subjects and, although demographic data such as participants' age and geographic region were collected, no personally identifiable information was solicited from participants. Participants completed a self-reported survey online, which took less than 15 minutes to complete. It must be noted that the questions were all presented on one continuous web page; implications regarding this survey type of construction are discussed in section 5.

As summarized in Table 1, Participants' Demographic Characteristics, age was stratified into three generational cohorts (GCOHORT). Observations ranged from 1.00 to 3.00 (18 years to 70 years). Millennials (the Generation Y cohort born 1981-1998) predominated (n = 75, 49.3%; SD = .721). More females than males participated in the study, (n = 97, 63.8%), and the majority of respondents had Bachelor degrees (n = 55, 36.2%; SD). The highest income range was $50,000 to $74,999 ($n$ = 49, 32.2%; SD = 1.93).

Table 1. Participants' Demographic Characteristics

	n	Percent
Age (GCOHORT)		
1981 – 1998, 18 – 35 yrs old (Generation Y/Millennial)	75	49.3%
1965 – 1980, 36 – 51 yrs old (Generation X)	55	36.2%
1946 – 1964, 52 – 70 yrs old (Baby Boomers)	22	14.5%
Gender		
Women	97	63.8%
Men	55	36.2%
Education		
Less than high school	1	0.7%
High school/GED equivalent	35	23.0%
Some college (no degree)	16	10.5%
Associates Degree	17	11.2%
Bachelor Degree	55	36.2%
Graduate or Professional Degree	28	18.4%
Income		
< $25,000	6	3.9%
$25,000 - $49,999	38	25.0%
$50,000 - $74,999	49	32.2%
$75,000 - $99,999	25	16.4%
> $99,999	34	21.1%
Refused to provide income information	2	1.3%

Note: N = 152

Most respondents were from the South Atlantic region of the US (*n* = 39, 25.7%), and the lowest regional representations were from the Mountain regions (*n* = 6, 3.9%). Nevertheless, all regions of the US were represented (Appendix A, Table 1).

3.3 Measures

Data on the DV, EISB, which is measured by file protection behavior (FPB), were collected on a five-point Likert-type single-item scale instrument. Single-item scales are appropriate when the construct it measures is clear, concrete, and unambiguous such that the question means the same thing to different raters (Diamantopoulos et al, 2012; Wanous et al., 1997). Study participants were asked "How important to you is it that only you or those you authorize are allowed to access the files of your organization". Responses were weighted *1* to *5* with lower scores implying lower file protection behavior. Instrument reliability is generally not calculated on single-item scales; however, based on Diamantopoulos et al (2012) and Wanous et al. (1997), these scales are considered reliable and valid when they measure a concrete, unambiguous construct; such is the case with the FPB scale in the present study.

Data on the IVs, personality traits, were collected with the public domain 50-item IPIP Big Five factors questionnaire instrument accessible at https://ipip.ori.org/new_ipip-50-item-scale.htm. Ten questions measured each of the five factors of personality traits. Responses to the 50-item IPIP Big Five Factors questionnaire instrument were measured on scales that ranged from 1 to 5, with 1 = *This is very inaccurate*, 2 = *This is inaccurate*, 3 = *This is neither inaccurate nor accurate*, 4 = *This is accurate*, and 5 = *This is very accurate*. Several items needed to be reversed scored (Table 3). Composite scores were obtained for the variables, which were renamed *Extra_Avg*, *Agree_Avg*, *Consc_Avg*, *EmStab_Avg*, and *Intell_Avg*. A further composite score of these renamed variables produced a single score for Overall Personality Traits (OPT). High scores on the 50-item IPIP Big Five factors questionnaire translates to higher expression of the personality trait.

The reliability and validity of the 50-Item IPIP instrument has long been established in prior research (e.g., Goldberg, 1993; Fronczyk, 2019; Lim & Ployhart, 2006; Robertson, Jangha, Piedmont, Sherman, & Williams, 2017; Rojas & Widiger, 2014). Psychometric properties of the instrument in the original Goldberg study indicated it exhibited very strong overall reliability ($\alpha = .84$). Overall reliability of the instrument in the present study was high, $\alpha = .78$ (Table 2). Differences in scale reliability between the original reports and those of the present study are attributed to sample size and composition.

Table 2. Original and Present Study 50-Item IPIP Instrument Reliability

Description	α (Original study)	Description	α (Present Study)
Overall scale reliability	α =.84	Overall scale reliability	α = .78
Extraversion	α = .87	Extraversion	α = .68
Agreeableness	α = .82	Agreeableness	α = .70
Conscientiousness	α = .79	Conscientiousness	α = .76
Emotional Stability	α = .86	Emotional Stability	α = .88
Intellect	α = 0.84	Intellect	α = .88

Data for generational cohort (GCOHORT) were taken from the demographic variables, which were collected to present an understanding of the population from which the sample was drawn. Study participants were asked, "The year you were born falls into which of the following age groups?" Responses ranged from *1* = 18 – 35 yrs old (1981 – 1998 Generation Y), *2* = 36 – 51 yrs old (1965 – 1980, Generation X), *3* = 52 – 70 yrs old (1946 – 1964, Baby Boomers). SPSS excluded from the analyses *1* = 18 – 35 yrs old (1981 – 1998, Generation Y).

3.4 Analysis of the Data

Examination of the research questions was by means of six hierarchical (a.k.a. *sequential*) multiple regressions (HMR) procedures; the HRM procedure is appropriate for assessing the additional contributions each variable makes to variances in the DV (Tabachnick & Fidell, 2007). The IBM® Statistical Package for the Social Sciences (SPSS) version 26 was used to analyze the data. To answer the theory-testing omnibus question (H_0), the variable *overall personality traits* (i.e., the composite score of the averaged scores for the variables measuring the five dimensions of the FFM) was first entered into the regression equation in Block 1. In a second step, the moderating generational age cohort variables, measured by span of years, were entered into the equation (Block 2). Similarly, to answer H_2 _ H_6, in five separate regression procedures, each of the five factors of personality traits variables (EACESI) was entered in Block 1 and the generational age variables were entered in Block 2 of the regression equation; these were regressed individually against the DV, FPB.

The Pearson's coefficient *R* was assessed to determine the direction and size of the magnitude of the relationship between the IVs and the DV. The Pearson product-moment correlation coefficient (*R*) is one type of effect size and is a standardized measure that provides information on the direction and strength of the relationship between two variables; this coefficient can range only from -1 through 0 = *no correlation*, to +1 = *a perfect linear correlation.* The *R* coefficient will always fall in the range of -1 to +1 (Sheskin 2010); the relationship between the tested IV and the DV is considered small effect when *R* =.10; medium or moderate effect when *R* = 30; and large effect when *R* = .50. The coefficient of determination, R^2, was appraised for the size of the effect contributed by the IV to variations in the DV. Per convention, statistical significance was set at $p < .05$. According to Cohen (1988), for *F*-tests multiple regressions, as indicated by R^2, a small effect size = .02, medium = .15, large = .35.

4. Results

The purpose of this study was to assess whether generational age cohort (GCOHORT) moderated the Big Five dimensions of personality traits (EACESI - IVs) and EISB to explain or predict FPB. Altogether, six hierarchical multiple regressions procedures were performed.

Personality traits have long been recognized as predictors of human behavior and for remaining stable over time (Costa, McCrae, & Löckenhoff, 2019; Gallagher, Fleeson, & Hoyle, 2010; McCrae & Costa, 1997), so the FFM was an appropriate theoretical model with which to underpin the study. The hierarchical multiple regressions statistical model applied to investigate relationships among the variables was also appropriate as it is useful for assessing the additional contributions each variable makes to variances in the DV, when the variables are entered into the regression equation sequentially. In other words, the main objective of hierarchical multiple regression analysis is to assess the proportion of the variation in the outcome variable explained by the addition of new independent variables. The means and standard deviations for the continuous variables are summarized in Appendix B, Table B1.

4.1 Distribution of the Responses in the Sample

To the question "*How important to you is it that you or those you authorize are allowed access to the files on your computer*", of the 152 participants surveyed, 70.4% (*n* = 107) indicated that it was very important or somewhat important (*n* = 32, 21.1%) to them. As mentioned previously, the raw personality traits scores were

averaged to obtain composite/mean scores for analysis. The personality traits with the highest mean expressions in the sample (Appendix B, Table B2) were agreeableness (n = 39, 25.7%), with highest scores reflecting high agreeableness (n = 24, 15.8%), and extraversion (n = 34). (n = 10, 6.6%), and the lowest was emotional stability (n = 4, 2.6%).

4.2 Results of the Test of the Null Hypotheses (H_0 – H_6)

Six hierarchical multiple regressions procedures were run to determine whether the addition of generational age to the regression equation improved the prediction of file protection behavior (FPB) over and above overall personality traits, extraversion, agreeableness, conscientiousness, emotional stability, and intellect. Two model summaries resulted from each of the tested IVs: the Model 1 Summary output represents the first step in the hierarchical analysis when only the main IV is used as a predictor. The Model 2 summary represents the full model results when generational age is entered into the equation in a second step; the main IV is also included in this output. In all cases, in the full model, the addition of generational age group to the regression equation did not contribute to a statistically significant relationship between any of the IVs and the DV ($p > .05$). Except for the regression of emotional stability (IV) against FPB ($p = .070$; $p > .05$), statistically significant relationships that ranged from fairly moderate to moderate existed between each of the remaining tested main IVs (i.e., overall personality traits, extraversion, agreeableness, conscientiousness, and intellect) and FPB. Full summaries of the results are presented in Table 3.

Table 3. Model Summary Results of Individual Level Big Five Personality Traits Analyses

Description (H_0, H_1)	Results
(**H_1**) Model 1: Predictor, Overall Personality Traits	$F(1,150) = 13.480$, $p = .000$ ($p < .05$); $R = .287$, $R^2 = .082$, $R^2adj. = .076$
(**H_2**) Model 1: Predictor, Extraversion	$F(1,150) = 11.833$, $p = .001$ ($p < .05$); $R = .270$, $R^2 = .073$, $R^2adj. = .067$
(**H_3**) Model 1: Predictor, Agreeableness	$F(1,150) = 8.471$, $p = .004$($p < .05$); $R = .231$, $R^2 = .053$, $R^2adj. = .047$
(**H_4**) Model 1: Predictor, Conscientiousness	$F(1,150) = 6.081$, $p = .015$ ($p < .05$); $R = .197$, $R^2 = .039$, $R^2adj. = .033$
(**H_5**) Model 1: Predictor, Emotional Stability	$F(1,150) = 3.338$, $p = .07$ ($p > .05$); $R = .148$, $R^2 = .022$, $R^2adj. = .015$
(**H_6**) Model 1: Predictor, Intellect	$F(1,150) = 14.124$, $p = .000$ ($p < .05$); $R = .293$, $R^2 = .086$, $R^2adj. = .080$

Note: p = .05

4.2.1 Overall Personality Traits (OPT), Generational Cohort vs. File Protection Behavior (H_1)

The F-ratio in the ANOVA Table indicated that the regression model was a good fit for the data, $F(1,150) = 13.48$, $p < .005$. Results of the present study agreed with evidence in the literature, which shows that, overall, personality traits explain or predict InfoSec behavior; in this case, FPB. In the present study, the strength of the relationship between OPT and FPB was positive, approximately medium ($R = .287$), and highly statistically significant (($p = .000$; $p < .001$). The IV (OPT) contributed 8.2% to the variation in the DV ($R^2 = .082$), which when adjusted, contributed to 7.6% (*Adjusted* $R^2 = .076$) of the variance in FPB. OPT added statistically significantly to the prediction of FPB; for each unit increase of OPT, there was a highly statistically significant 38% increase in FPB (ß = .380; $p = .000$, $p < .001$). However, the full model of OPT and generational age to predict FPB was not statistically significant ($R^2 = .092$; $p = .47$, $p > .05$). Hypothesis one (H_1), which stated that generational cohort will moderate the relationship between overall personality traits and FPB, was not supported.

4.2.2 Extraversion, Generational Cohort vs. File Protection Behavior (H_2)

The strength of the correlation between extraversion and FPB was positive, fairly moderate ($R = .270$), and was statistically significant ($p = .00$; $p < .01$). The size of the contribution made by the extraversion personality trait to the variance in FPB was 7.3% ($R^2 = .073$); when adjusted, this contribution accounted for 6.7% of the variance in FPB (*Adjusted* $R^2 = .067$). Extraversion added statistically significantly to the prediction of FPB, $\mathbf{F}(1,150) = 11.8333$, $\mathbf{p} < .05$, $\mathbf{R^2} = .073$. For each unit increase of the extraversion trait, there was a statistically significant 25.9% increase in FPB (ß = .259; $p = .001$; $p < .05$). The full model of extraversion and generational age to predict FPB was not statistically significant ($R^2 = .072$; $p = .345$, $p > .05$). Hypothesis two (H_2), which stated that generational cohort will moderate the relationship between extraversion and employee's InfoSec behavior, as measured by file protection behavior, was not supported.

4.2.3 Agreeableness, Generational Cohort, vs. File Protection Behavior (H_3)

The correlation between agreeableness and FPB was positive, somewhat moderate (R = .231), was statistically significant (p = .004, p < .05), and contributed 5.3% (R^2 = .053) of the variance in FPB. When adjusted, this contribution amounted to 4.7% (*Adjusted* R^2 = .047). Agreeableness added statistically significantly to the prediction of FPB, **F**(1,150) = 6.183, **p** < .05, $\mathbf{R^2}$ = .053. For each unit increase of the agreeableness trait, there was a statistically significant 23.5% increase in FPB (ß = .235; p = .004, p < .05). The full model of agreeableness and generational age to predict FPB was not statistically significant (R^2 = .066; p = .373, p > .05). Hypothesis three (H_3), which stated that generational cohort will moderate the relationship between agreeableness and employee's InfoSec behavior, as measured by file protection behavior, was not supported.

4.2.4 Conscientiousness, Generational Cohort, vs. File Protection Behavior (H_4)

The strength of the correlation between conscientiousness and FPB was fairly weak, and statistically significant (R = .197; p = .015; p < .05). Conscientiousness contributed 3.9% of the variance in FPB (R^2 = .039). When adjusted, this contribution amounted to 2.8% (*Adjusted* R^2 = .028). The conscientiousness trait added statistically significantly to the prediction of FPB, **F**(1,150) = 6.081, p = .015, **p** < .05; $\mathbf{R^2}$ = .039. There was a positive relationship between conscientiousness and FPB such that for each unit increase of the conscientiousness trait there was a statistically significant 24.3% increase in FPB (ß = .243; p = .015, p < .05). The full model of OPT and generational age to predict FPB was not statistically significant (R^2 = .197; p = .529, p > .05). Hypothesis four (H_4), which stated that generational cohort will moderate the relationship between conscientiousness and employee's InfoSec behavior, as measured by file protection behavior, was not supported.

4.2.5 Emotional Stability, Generational Cohort, vs. File Protection Behavior (H_5)

The strength of the correlation between emotional stability and FPB was weak (R = .148), positive, and statistically nonsignificant (*R2 = .022; p* = .070), contributing a mere 2.2% to variation in the DV. Although it neared statistical significance (p = .07), the emotional stability trait did not statistically significantly add to the prediction of FPB, **F**(1,150) = 3.338, p = .070, **p** > .05; $\mathbf{R^2}$ = .022. The full model of emotional stability and generational age to predict FPB was not statistically significant (R^2 = .022; p = .587, p > .05). Hypothesis five (H_5), which stated that generational cohort will moderate the relationship between emotional stability and employee's InfoSec behavior, as measured by file protection behavior, was not supported.

4.2.6 Intellect, Generational Cohort, vs. File Protection Behavior (H_6)

The correlation between intellect and FPB was positive, moderate, and statistically significant (R = .293; p = .000, p < .01). Intellect contributed to 8.6% of the variance in FPB (R^2 = .086). When adjusted, this contribution amounted to 8% (*Adjusted* R^2 = .080). The intellect trait added statistically significantly to the prediction of FPB, **F**(1,150) = 14.124, p = .000, **p** < .001; $\mathbf{R^2}$ = .093 . There was positive relationship between intellect and FPB such that for each unit increase of the intellect trait, there was a highly statistically significant 34.1% increase in FPB (ß = .341; p = .000; p < .001). The full model of intellect and generational age to predict FPB was not statistically significant (R^2 = .093; p = .580, p > .05). Hypothesis six (H_6), which stated that generational cohort will moderate the relationship between intellect and employee's InfoSec behavior, as measured by file protection behavior, was not supported.

5. Discussion

Our hypotheses that generational age cohorts (GCOHORT) will influence (moderate) the relationship between the Big Five dimensions of personality traits and employees' InfoSec behaviors, which was measured by file protection behavior, was not supported. There are differences in how diverse generations respond to their environments and these responses affect functioning in the workplace (Scroxton, 2020), but while our findings confirmed that the FFM has the power to explain or predict employees' InfoSec (file protection) behavior, in no instance did generational GCOHORT exert a statistically significant influence on the relationship between the five factors of personality (i.e., extraversion, agreeableness, conscientiousness, emotional stability, and intellect [EACESI]) and employees' file protection behavior. This result was supported in the literature by McCormac et al. (2016), who reported positive relationships between the Big Five factors of personality traits and InfoSec activities, but no statistically significant relationship between age and InfoSec activities; yet, contrary to findings in the present study and McCormac et al., other inquiries revealed statistically significant relationships between personality, various age groups, and risky behaviors—including risky InfoSec behaviors (e.g. Nicholson et al., 2005; Pattinson et al., 2012, 2015; Shappie et al, 2019).

Millennials (1981–1998) generally exhibited responsible InfoSec behaviors in relation to phishing and spamming, but lower InfoSec awareness in regards to malware, viruses, worms, and Trojans. Consequently, their

use of personal devices for work, access to social media at work, and their perceptions about file sharing was worrisome (Hardy, 2016). Similar concerns were expressed by Garba et al. (2015) regarding the use of personal devices by Generation X (1965–1980), as they were more dependent on their personal devices in the workplace. Older individuals were shown to be generally more cautious and less prone to risk-taking (Nicholson et al., 2005), a finding confirmed by Pattinson et al. (2015) and McCormac et al. (2016) who reported that older individuals were more likely to engage in less risky InfoSec behaviors. Given the evidence concerning generational age and InfoSec behaviors, it was surprising that the findings in the present study indicated no effect of GCOHORT on the relationship between EACESI and FPB.

Another surprise finding in the present study was that of the nonsignificant effect of emotional stability trait on file sharing behavior, as the contrary is documented in the literature (e.g. Li et al, 2014; Nicholson et al., 2005;). A close examination of the raw data revealed a significant lack of variation in the responses to the questions related to the emotional stability trait. This lack of variability may have been due to fatigue or boredom when answering the questions, which, perhaps, could be attributable to the design construction of the survey, as previously mentioned in section *3.2* and described in the *Limitations* section. A fairly high number of employees in the sample expressed ambivalence about the emotional stability trait by choosing a neutral response (i.e., *3 = this is neither accurate nor inaccurate*) to the emotional stability questions. Nevertheless, a valuable insight that emerged from the study is that, although there has been a lingering perception that older employees are more prone to risky InfoSec behaviors online (Chakraborty, et al., 2013), evidence in the literature seems to suggest otherwise (e.g., Pattinson et al, 2015; McCormac et al., 2016).

6. Limitations

The strength of the study was evident in the heterogeneous composition of the sample due to the age, gender, income, educational, and regional diversity of the national sample of employees who had access to sensitive files in their organization, which improved the generalizability of the study. However, since the study was conducted in the U.S. among a sample (N = 152) based on specific inclusion and exclusion criteria, the results cannot be generalized beyond the U.S. based sample as cultural or socio-economic differences among different countries might produce different results. Secondly, the age boundary (18 – 70) precluded younger and older individuals. According to the Bureau of Labor Statistics, many individuals in the U.S. enter the workforce below the age of 18 and stay in the workforce beyond the age of 70; excluding this population from the study may not have revealed the true effect of generational age on FSB. In fact, the Boomer generation was underrepresented in the sample, and this may have skewed results of the study. Additionally, unemployed and part-time workers were excluded from the study; it is not known whether any of these workers are related to the so-called "gig economy", and whether the transient nature of their employment might have an effect on their perceptions of their file protection InfoSec behaviors. Inquiries in these areas might be considered.

Several other limitations must be acknowledged. First, the self-report nature of the data may have biased the study in several ways. For example, the truthfulness of the responses could not be verified (Emerson, Felce, & Stancliffe, 2013). Uncertainty concerning whether their responses could be used against them could cause respondents to choose self-favoring responses. Self-reported data presents a risk to validity (Rosenbaum, Rabenhorst, Reddy, Fleming, & Howells, 2006). However, the guarantee of anonymity in data collection could have mitigated this threat to validity; additionally, *in situ* studies on the phenomenon might provide deeper insights.

Thirdly, the construction and presentation of the online survey may have biased the responses gravely by causing fatigue amongst the respondents, since all of the questions were presented in one long unbroken webpage. Questionnaires of unbroken length are considered poor as they provoke boredom and mental fatigue in respondents (Foddy, 1993). Additionally, respondents can easily forget instructions posted at the top of the page, omit responses, or provide non-substantive responses with no variability (Ganassali, 2008). In the data used in this study, there was no variability in several of the responses.

7. Conclusion and Future Directions

Based on results of the present study, with the exception of emotional stability, personality traits were better predictors of employees' file protection behaviors than employees' generational age cohort. The literature revealed that certain personality types, and combination of personality types, were predictive of higher or poorer levels of InfoSec behaviors (e.g. Halevi et al., 2013; McCormac et al, 2016; Pattinson et al, 2015; Shappie et al., 2019; Welk, et al., 2015); however, there are conflicting reports about personality traits and their relationship to InfoSec. Admittedly, the behavioral approach to understanding InfoSec behaviors is still developing so more research is needed in this area to bring clarity to the role that personality plays in information security behaviors

such as, among others, file protection behavior.

While we are not suggesting that personality traits should be the sole consideration used to determine whether one employee might be a greater Info-Sec risk than another, we do suggest that results of this study revealed areas of concern regarding InfoSec behaviors that can be explored further. For example, since evidence in the literature is that individuals' personal behaviors at home do not change in the workplace (e.g., Li et al., 2014), and since many employees are now working from home due to COVID-19, it is reasonable to surmise that the results obtained from this study regarding employees' file protection behavior at work is reflective of such behavior at home, and *vice versa*. Due to the prevalence of at-home workers attributed to the COVID-19 pandemic, further studies might be warranted to compare onsite workers and work-from-home employees as results might reveal whether modifications to InfoSec training might be necessary. Given the gravity of insecure Info-Sec behavior, perhaps organizations' training efforts might include conscious behavior modification efforts for—especially as home based employees might have more opportunities to engage in social media activities; these activities have been shown to be related to risky InfoSec behaviors. It might be beneficial to employees to understand their dominant personality traits and how these traits might affect their attitudes toward InfoSec behaviors. Frequent reinforcement of training that includes role-playing in risky and/or healthy InfoSec behaviors might be beneficial to companies wishing to prioritize and promote InfoSec behaviors among their employees.

Other types of analytical approaches might provide a deeper understanding of the problem, and other types of independent variables, including different demographic variables, might be examined for their effect on different types of InfoSec behaviors. For example, traits might be tested for possible interaction effects on the relationship between personality traits, FPB, or other specific types of employee InfoSec behaviors—especially since only one general aspect of employee InfoSec behavior was examined in the present study. (i.e., file protection behavior). Such studies might provide a more granular and comprehensive understanding of whether there are types of InfoSec behaviors that are more or less affected by personality traits' interaction with each other or other possible moderating influences such as gender, education, job satisfaction, length of employment, etc.

Finally, given the potential gravity of the possible negative effects of the construction and presentation of the online questionnaire, the study might be replicated with a better constructed survey using several short web pages on which questions from a single personality subscale (e.g. items for each of the personality traits) are grouped.

References:

Allik, J., Church, A. T., Ortiz, F. A., Rossier, J., Hřebíčková, M., de Fruyt, F., … McCrae, R. R. (2017). Mean profiles of the NEO personality inventory. *Journal of Cross-Cultural Psychology*, *48*(3), 402–420. https://doi.org/10.1177/0022022117692100

Allport, G. W. (1927). Concepts of traits and personality. *Psychological Bulletin, 24*, 284-293. https://doi.org/10.1037/h0073629

American Psychological Association. (2020). *Personality.* Retrieved from https://www.apa.org/topics/personality

Barrick, M. R., Mount, M. K., & Gupta, R. (2003). Meta-analysis of the relationship between the five-factor model of personality and Holland's occupational types. *Personnel Psychology, 56*(1), 45-74. https://doi.org/10.1111/j.1744-6570.2003.tb00143.x

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security, 23*(3), 253-264. https://doi.org/10.1016/j.cose.2003.09.002

Budzak, D. (2016). Information security–the people issue. *Business Information Review*, *33*(2), 85-89. https://doi.org/10.1177/0266382116650792

Bureau of Labor Statistics. (2014, 2017). Share of labor force projected to rise for people age 55 and over and fall for younger age groups. *The Economics Daily.* Retrieved from http://www.bls.gov/opub/ted/2014/ted_20140124.htm

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems, 5*5(4), 948-956. https://doi.org/10.1016/j.dss.2013.01.004

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39, Part B*(0), 447-459. https://doi.org/10.1016/j.cose.2013.09.009

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of Information Science*, *44*(6), 752-767. https://doi.org/10.1177/0165551517748288

Clement, J. (2020). Percentage of baby boomers who use selected social networks as of February, 2019. *Statistica.* Retrieved from https://www.statista.com/statistics/436417/us-baby-boomer-selected-social-networks/

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

Colwill, C. (2009). Human factors in information security: The insider threat – who can you trust these days? *Information security Technical Report.* https://doi.org/10.1016/j.istr.2010.04.004

Costa, P. T., & McCrae, R. R. (1992). *Revised NEO Personality Inventory (NEO-PI-R) and NEO Five Factor Model (NEO-FFI) Professional manual.* Odessa, FL: Psychological Assessment Resources.

Costa, P. T., Jr., McCrae, R. R., & Löckenhoff, C. E. (2019). Personality across the life span. *Annual Review of Psychology, 70*, 423-448. https://doi.org/10.1146/annurev-psych-010418-103244

Costa, P. T., McCrae, R. R., & Kay, G. G. (1995). Persons, Places, and Personality: Career Assessment Using the Revised NEO Personality Inventory. *Journal of Career Assessment, 3*(2), 123-139. https://doi.org/10.1177/106907279500300202

Damian, R. I., Spengler, M., Sutu, A., & Roberts, B. W. (2019). Sixteen going on sixty-six: A longitudinal study of personality stability and change across 50 years. *Journal of Personality and Social Psychology, 117*(3), 674-695. https://doi.org/10.1037/pspp0000210

Diamantopoulos, A., Sarstedt, M., Fuchs, C., Wilczynski, P., & Kaiser, S. (2012). Guidelines for choosing between multi-item and single-item scales for construct measurement: a predictive validity perspective. *Journal of the Academy of Marketing Science, 40*(3), 434-449. https://doi.org/10.1007/s11747-011-0300-3

Duchscher, J. E., & Cowin, L. (2004). Multigenerational nurses in the workplace. *Journal of Nursing Administration, 34*(11), 493-501. https://doi.org/10.1097/00005110-200411000-00005

Emerson, E., Felce, D., & Stancliffe, R. J. (2013). Issues concerning self-report data and population-based data sets involving people with intellectual disabilities. *Intellectual and Developmental Disabilities, 51*(5), 333-348. https://doi.org/10.1352/1934-9556-51.5.333

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian universities. *Journal of Physics: Conference Series, 1339*, 012098. https://doi.org/10.1088/1742-6596/1339/1/012098

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods, 41*, 1149-1160. https://doi.org/10.3758/BRM.41.4.1149

Foddy, W. (1993). *Constructing questions for interviews and questionnaires: Theory and practice in social research*. Cambridge, UK. Cambridge University Press. https://doi.org/10.1017/CBO9780511518201

Fronczyk, K. (2019). Congruence and measurement invariance of self-report and informant-ratings of the Big Five dimensions. *Personality and Individual Differences, 139*, 7-12. https://doi.org/10.1016/j.paid.2018.10.036

Gallagher, P., Fleeson, W., & Hoyle, R. H. (2010). A Self-Regulatory Mechanism for Personality Trait Stability. *Social Psychological and Personality Science*, 2(4), 335-342. https://doi.org/10.1177/1948550610390701

Ganassali, S. (2008). The influence of the design of web survey questionnaires on the quality of responses. *Survey Research Methods, 2*(1), 31-32.

Garba, A. B., Armarego, J., & Murray, D. (2015). Bring your own device organizational information security and privacy. *ARPN Journal f Engineering and Applied Sciences*, 1279-1287. Retrieved from https://researchrepository.murdoch.edu.au/id/eprint/25699/1/bring_your_own_device.pdf

Goddijn, I. (2019). Cyber risk analytics: 2019 Mid-year quick view data breach. *Riskbased Security.* Retrieved from https://bit.ly/3gAHN9h

Goddijn, I., & Kouns, J. (2020). 2020 Q1 report, data breach quick review. *RiskBased Security.* Retrieved from https://pages.riskbasedsecurity.com/

Goldberg, L. R. (1993). The structure of phenotypic personality traits. *American Psychologist, 48*(1), 26-34. https://doi.org/10.1037/0003-066X.48.1.26

Goldberg, L. R. (1999). A broad-bandwidth, public domain, personality inventory measuring the lower-level facets of several five-factor models. In I. Mervielde, I. Deary, F. De Fruyt, & F. Ostendorf (Eds.), *Personality Psychology in Europe*, Vol. 7 (pp. 7-28). Tilburg, The Netherlands: Tilburg University Press.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2017). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. https://doi.org/10.1016/j.cose.2017.11.015

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of Internet hazards. *Educational Gerontology, 36*(3), 173-192. https://doi.org/10.1080/03601270903183065

Haddington, L. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1). Retrieved from https://www.cybercrimejournal.com/HadlingtonVol12Issue1IJCC2018.pdf

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2383427

Hardy, K. W. (2016). Millennials bring new workplace cybersecurity challenges. *SHRM*. Retrieved from https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/millennials-bring-new-workplace-cybersecurity-challenges.aspx

Hayden, L. (2009). Human Information Security Behaviors: Differences across Geographies and Cultures in a Global User Survey. *Proceedings of the American Society for Information Science and Technology, 46*(1). https://doi.org/10.1002/meet.2009.145046022

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2). https://doi.org/10.1016/j.dss.2009.02.005

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, *51*(1), 69-79. https://doi.org/10.1016/j.im.2013.10.001

Jackson, J. J., Bogg, T., Walton, K. E., Wood, D., Harms, P. D., Lodi-Smith, J., … Roberts, B. W. (2009). Not all conscientiousness scales change alike: A multimethod, multisample study of age differences in the facets of conscientiousness. *Journal of Personality and Social Psychology, 96*(2), 446-459. https://doi.org/10.1037/a0014156

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: evidence from a multichannel retailer. *Journal of Marketing, 82*(2), 85-105. https://doi.org/10.1509/jm.16.0124

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC).* https://doi.org/10.1109/CIC48465.2019.00047

Jeske, D., Briggs, P., & Coventry, L. (2016). Exploring the relationship between impulsivity and decision-making on mobile devices. *Personal and Ubiquitous Computing, 20*(4), 545-557. https://doi.org/10.1007/s00779-016-0938-4

Johansen, A. G. (2020). *10 cybersecurity best practices that every employee should know.* Retrieved from https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html

Johansen, A. G. (2020). *10 cybersecurity best practices that every employee should know.* Retrieved from https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2019). Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics Journal, 26*(1), 461-473. https://doi.org/10.1177/1460458219832048

Lahcen, R. A. M, Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity, 3*(1). https://doi.org/10.1186/s42400-020-00050-w

Leszczyna, R. (2013). Cost assessment of computer security activities. *Computer Fraud & Security, 2013*(7),

11-16. https://doi.org/10.1016/S1361-3723(13)70063-0

Li, L., Li., A., Hao, B., Guan, Z., & Zhu, T. (2014). Predicting active users' personality based on micro-blogging behaviors. *PLoS ONE, 9*(1), e84997. https://doi.org/10.1371/journal.pone.0084997

Lim, B. C., & Ployhart, R. E. (2006). Assessing the convergent and discriminant validity of Goldberg's International Personality Item Pool: A multitrait-multimethod examination. *Organizational Research Methods, 9*(1), 29-54. https://doi.org/10.1177/1094428105283193

Madden, M. (2010). Older adults and social media. *Pew Internet & American Life Project, 27.* Retrieved from http://pewInternet.org/Reports/2010/Older-Adults-and-Social-Media.aspx

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36-58. https://doi.org/10.1509/jm.15.0497

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2016). Individual differences and Information Security Awareness. *Computers in Human Behavior, 69*, 151-156. https://doi.org/10.1016/j.chb.2016.11.065

McCrae, R. R., & Costa, P. T. (1997). Personality trait structure as a human universal. *American Psychologist, 52*(5), 509-516. https://doi.org/10.1037/0003-066X.52.5.509

McGhee, R. L., Ehrler, D. J., Buckhalt, J. A., & Phillips, C. (2012). The relation between Five-Factor Personality Traits and risk-taking behavior in preadolescents. *Psychology, 03*, 558-561. https://doi.org/10.4236/psych.2012.38083

Nicholson, N., Soane, E., Fenton-O'Creevy, M., & Willman, P. (2005). Personality and domain-specific risk taking. *Journal of Risk Research, 8*(2), 157-176. https://doi.org/10.1080/1366987032000123856

Ornstein, C., & Huseman, J. (2015). Inappropriate social media posts by nursing home workers, detailed. *ProPublica.org.* Retrieved from https://www.propublica.org

Osborne, J. W., & Waters, E. (2002). Four assumptions of multiple regression that researchers should always test. *Practical Assessment, Research & Evaluation, 8*(2). Retrieved from http://pareonline.net

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31*(5), 673-680. https://doi.org/10.1016/j.cose.2012.04.004

Patsiotis, A. G., Hughes, T., & Webber, D. J. (2013). An examination of consumers' resistance to computer-based technologies. *The Journal of Services Marketing, 27*(4), 294-311. https://doi.org/10.1108/08876041311330771

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security behavior: An Australian web-based study. *Human Aspects of Information Security, Privacy, and Trust*, 231-241. https://doi.org/10.1007/978-3-319-20376-8_21

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security, 20*(1), 18-28. https://doi.org/10.1108/09685221211219173

Peikari, H. R., & Banazdeh, B. (2019). The relationship between information security awareness and the intention to violate information security with the mediating role of individual norms and self-control. *Security & Social Order Strategic Studies, 7*(4), 7-9. https://doi.org/10.22108/ssoss.2019.108446.1174

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611. https://doi.org/10.1016/j.cose.2011.12.010

Rafter, D. (2020). 2019 data breaches: 4 billion records breached so far. *Norton.* Retrieved from https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

Rahman, S. M. A. K., Sathik, M. M., & Kannan, K. S. (2012). Multiple linear regression models in outlier detection. *International Journal of Research in Computer Science, 2*(2), 23-28. https://doi.org/10.7815/ijorcs.22.2012.018

Roberts, B. W., & Mroczek, D. (2008). Personality trait change in adulthood. *Current Directions in Psychological Science, 17,* 31-35. https://doi.org/10.1111/j.1467-8721.2008.00543.x

Robertson, T. M., Jangha, A., Piedmont, R. L., Sherman, M. F., & Williams, J. E. (2017). Factor structure and personality disorder correlates of responses to the 50-Item IPIP Big Five Factor marker scale. *Journal of Social Research & Policy, 8*(2).

Rojas, S. L., & Widiger, T. A. (2014). Convergent and discriminant validity of the five factor form. *Assessment, 21*(2), 143-157. https://doi.org/10.1177/1073191113517260

Rosenbaum, A., Rabenhorst, M. M., Reddy, M. K., Fleming, M. T., & Howells, N. L. (2006). A comparison of methods for collecting self-report data on sensitive topics. *Violence and Victims, 21*(4), 461-71. https://doi.org/10.1891/0886-6708.21.4.461

Russell, J. D., Weems, C. F., Ahmed, I., & Golden, G. R. III. (2017). Self-reported secure and insecure cyber behaviour: facture structure and associations with personality factors. *Journal of Cyber Security Technology, 1*(3-4), 163-174. https://doi.org/10.1080/23742917.2017.1345271

Scroxton, A. (October 2020). Over-30s tend to do better at cyber security than younger colleagues. *Computer Weekly.* Retrieved from https://www.computerweekly.com/news/252472594/Over-30s-tend-to-do-better-at-cyber-security-than-younger-colleagues

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media Culture*. Advance online publication. https://doi.org/10.1037/ppm0000247

Shepherd, M. M., & Klein, G. (2012). Using deterrence to mitigate employee internet abuse. *2012 45th Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2012.627

Sheskin, D. (2010). Correlation. In Neil J. Salkind (Ed.), *Encyclopedia of Research Design.* (pp. 265-268). Thousand Oaks, CA: SAGE.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Explaining initial adoption of information security behavior. *Computers & Security, 49*(0), 177-191. https://doi.org/10.1016/j.cose.2015.01.002

Shropshire, J., Warkentin, M., Johnson, A.C., & Schmidt, M.B. (2006). Personality and IT security: An application of the five-factor model. *Proceedings of the twelvth Americas conference on information systems Acapulco, Mexico,* 3443-3449. Retrieved from https://aisel.aisnet.org/

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security, 25*(5), 494-534. https://doi.org/10.1108/ICS-07-2016-0054

Syed, J., & Tappin, R. M. (2019). IT professionals' personality, personal characteristics, and commitment: Evidence from a national survey. *Computer and Information Science, 12*(3), 58. https://doi.org/10.5539/cis.v12n3p58

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics* (5th ed.). Boston: Pearson Education, Inc.

Thompson, K., & von Solms, R. (2005). Information security obedience: A definition. *Computers & Security, 24*(1), 69-75. https://doi.org/10.1016/j.cose.2004.10.005

Toossi, M., & Torpey, E. (2017). Older workers: Labor force trends and career options. *U.S. Bureau of Labor Statistics.* Retrieved from https://www.bls.gov/careeroutlook/2017/article/older-workers.htm

Uffen, J., Kaemmerer, N., & Breitner, M. H. (2013). Personality traits and cognitive determinants–an empirical investigation of the use of smartphone security measures. *Journal of Information Security, 4*(4), 203-212. https://doi.org/10.4236/jis.2013.44023

Uffen, J., Guhr, N., & Breitner, M. H. (2012). Personality traits and information security management: An empirical study of information security executives. In *International Conference on Information Systems, ICIS 2012* (Vol. 2, pp. 1188-1209). Orlando, FL.

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 123*, 29-39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Villafranca, E. (2015). Exploring millennials' malware awareness and intention to comply with information security policy. *Review of Integrative Business & Economics Research*, 153-161. Retrieved from http://buscompress.com/uploads/3/4/9/8/34980536/riber_b15-156__153-161_.pdf

von Solms, B., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers &*

Security, 23(3), 191-198. https://doi.org/10.1016/j.cose.2004.01.012

Wanous, J. P., Reichers, A. E., & Hudy, M. J. (1997). Overall job satisfaction: How good are single-item measures? *Journal of Applied Psychology, 82*(2), 247-252. https://doi.org/10.1037/0021-9010.82.2.247

Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2015).Will the phisher-men reel you in? *International Journal of Cyber Behavior Psychology and Learning, 5*(4), 1-17. https://doi.org/10.4018/IJCBPL.2015100101

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Cyberpsychology, behavior, and social networking. *Mary Ann Liebert, Inc. 18*(1), 3-7. https://doi.org/10.1089/cyber.2014.0179

Wilner, A. S. (2018). Cybersecurity and its discontents: Artificial intelligence, the Internet of things, and digital misinformation. *International Journal, 73*(2), 308-316. https://doi.org/10.1177/0020702018782496

Zemke, R., Raines, C., & Filipczak, B. (2000). *Generations at work.* New York: Amazon.

Zhen, J., Xie, Z., & Dong, K. (2020). Relationship between information security behavior and satisfaction degree of psychological needs and the mediation effect of team effectiveness and organizational commitment. *Revista Argentina De Cl ínica Psicol ógica, 29*(1), 442.

Appendix A

Table A1. Geographic Distribution of the Sample

	Description of Region	*n*	Percentage
1	New England (Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, Connecticut)	7	4.6%
2	Middle Atlantic (New York, New Jersey, Pennsylvania)	24	15.8%
3	East North Central (Ohio, Indiana, Illinois, Michigan, Wisconsin)	20	13.2%
4	West North Central (Minnesota, Iowa, Missouri, North Dakota, South Dakota, Nebraska, Kansas)	12	7.9%
5	South Atlantic (Delaware, Maryland, District of Columbia, Virginia, West Virginia, North Carolina, South Carolina, Georgia, Florida)	39	25.7%
6	East South Central (Kentucky, Tennessee, Alabama, Mississippi)	10	6.6%
7	West South Central (Arkansas, Louisiana, Oklahoma, Texas)	16	10.5%
8	Mountain (Montana, Idaho, Wyoming, Colorado, New Mexico, Arizona, Utah, Nevada)	6	3.9%
9	Pacific (Washington, Oregon, California, Alaska, Hawaii)	18	11.8%
10	I do not live in the United Sates	0	0%

Note: N = 152

Appendix B

Table B1. Continuous Variables: Means and Standard Deviations

Variable	*M*	*SD*	*N*
18 – 35 yrs old (Generation Y,1981 – 1998)	.49	.502	152
36 – 51 yrs old (Generation X, 1965 – 1980)	.36	.482	152
52 – 70 yrs old (Baby Boomers, 1946 – 1964)	.14	.353	152
File Protection Behavior	1.45	.875	152
Overall Personality Traits	3.58	.661	152
Extraversion (factor 1)	3.32	.912	152
Agreeableness (factor 2)	3.89	.861	152
Conscientiousness (factor 3)	3.62	.711	152
Emotional Stability (factor 4)	3.33	.959	152
Intellect (factor 5)	3.73	.753	152

Table B2. Distribution of the Mean Scores of Responses in the Sample

Response Range	E*	%	A*	%	C*	%	E-S*	%	I*	%
1 = this is very inaccurate	2	1.3	2	1.3	0	0.0	0	0.0	1	0.7
2 = This is moderately inaccurate	2	1.3	1	0.7	0	0.0	3	2.0	0	0.0
3 = This is neither accurate nor inaccurate	16	10.5	5	3.3	4	2.6	10	6.6	9	5.9
4 = This is moderately accurate	4	2.6	7	4.6	7	4.6	7	4.6	9	5.9
5 = This is very accurate	10	6.6	24	15.8	5	3.6	4	2.6	9	5.9
Total	*n*=34	22.3	*n*=39	25.7	*n*=16	10.8	*n=24*	15.8	*n=28*	*18.4*

Notes: *E = Extra_Ave, *A = Agree_Avg, *C = Consc_Avg, *E-S = EmStab_Avg, *I = Intell_Avg

**Personality traits scores were averaged to obtain composite scores for analysis; shown are the totals of the mean scores.