2023

Generational Information Security Awareness and the Role of Big Five Personality Traits

Gloria McCue
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral dissertation by

Gloria McCue

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Richard Thompson, Committee Chairperson, Psychology Faculty
Dr. Barbara Chappell, Committee Member, Psychology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2023

Abstract

Generational Information Security Awareness and the Role of Big Five Personality Traits

by

Gloria McCue

MS, Oklahoma State University, 2009

BS, University of Oklahoma, 2005

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Industrial and Organizational Psychology

Walden University

August 2023

Abstract

Technological change drives organizations to safeguard information systems. However, such safeguards are dependent upon people to follow security rules. This study examined generational cohorts and personality traits and their impact on information security awareness. Participants in this study were 137 volunteers who completed an anonymous survey online. Two tools were utilized to collect data from the participants: the Human Aspects of Information Security Questionnaire and the Big Five Inventory, which captured behaviors and personality traits, respectively. The three main generational cohorts represented in the study, Baby Boomers, Generation X, and Generation Y, were in today's workforce. The results of the study indicated that generational cohort had no bearing on information security awareness or other security outcomes. In terms of the five factor model of personality, conscientiousness and openness were related to information security awareness. Specifically, effective training was lacking in individual security awareness. Positive social change implications may be evident through providing strategies to promote better programs that could raise organization commitment of generational cohorts. Increased awareness to personality traits and being aware of hampered information, supports both individuals and corporations from compromised situations. Organizations can utilize those two factors toward positive security awareness posture.

Generational Information Security Awareness and the Role of Big Five Personality Traits

by

Gloria McCue

MS, Oklahoma State University, 2009

BS, University of Oklahoma, 2005

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Organizational Psychology

Walden University

August 2023

Dedication

This dissertation is dedicated to our Heavenly Father, Jesus Christ, as well as my family and friends that have supported me through my schooling to its completion.

Acknowledgments

Thank you, Dr. Rich Thompson, for your guidance and making things understandable throughout this process. A special thank you to my family and friends that have supported me through my schooling to its completion. And thank you mom for instilling education as an important factor in my life and supporting me while you were here with our family.

Table of Contents

List of Tables

Chapter 1: Introduction to the Study

Lack of security awareness has consequences for organizations and individuals (Ande et al., 2019; Weber & Horn, 2017). In the United States, organizations and individuals struggled with cyberattacks, information and identity theft on a daily basis. There are numerous threats to security and growing daily. Cyber threats involve multiple age groups and are considered social engineering, which introduces threats by the use of telephone calls, phishing emails, text, or malware into networks and computer systems (Cunningham et al., 2018).

During 2016, security experts noted 67,000 new malware threats are found on the Internet every day (Jenab & Moslehpour, 2016). Additional research from Torten et al. (2018) showed the growing concern for corporations as breaches of information caused damage to reputation, performance, and compromise to intellectual property. The frequency, sophistication, and impact of cyberattacks against firms continued to increase and showed no sign of diminishing despite the efforts to improve cyber-defenses (Beuran et al., 2018; Jeong et al., 2019; Malatji et al., 2020; Zimmermann & Renaud, 2019;).

Prior research demonstrated the relationship between cybersecurity issues and personality traits (Marangione, 2019; Shappie et al., 2019). The weakest link organizations face regarding data integrity is people Parsons et al., 2017a). Security surveys and reports showed that employees are a dominant source of breaches, resulting in approximately 95% of security incidents from human error (Parsons et al., 2017a; Pricewaterhouse Coopers, 2014, 2015; Parsons et al., 2014b). Parsons et al. (2014b), Pattinson et al. (2019) and McCormac et al. (2017) evaluated personality traits in

individuals that found conscientiousness and agreeableness had the highest association with information security. There was minimal research focused on the personality traits in the five working generations and how these personalities might impact information security (Thompson et al., 2017). Consideration on personality traits of generational cohorts combined with information security awareness, focus on the prominent elements found in one's personality can help develop workplace solutions.

The millennial generation has utilized news outlets and social media to release sensitive information which has caused security challenges (Marangione, 2019). Baby boomers and the silent generation tend to have greater safety concerns regarding online security, relying on others for assistance and are less confident in the use of protection as compared to their millennial counterparts (Jiang et al., 2016).

Understanding the role of people, specifically personality and generations, on internet security has potential social change implications. Technology has changed interactions, the use of information, and business dealings. This study implicates social change in the areas of increased awareness about the impact of personality traits and hampered information security awareness to both individuals and corporations for compromised situations. The research results provided knowledge useful in designing or implementing programs that focus specifically on the traits for each generational cohort to enable an increased awareness. Approaching positive social change by considering the personality traits in generational cohorts and helping individuals understand the specific deficiencies lead to the correction of information security awareness.

Chapter 1 contains a description of the five-factor personality traits used to predict information security awareness of generational cohorts. The Background section summarizes the literature relating to generational cohorts, personality traits, and information security and addressed the current knowledge gap. In the Problem Statement section, I discuss the problem's evidence and point to how the situation is relevant and significant. The Purpose section provides information that functions as a connection to the issue addressed. The Research Questions and Hypotheses section includes the predictor and criterion variables. The Conceptual Framework section proposes the theories studied—generational cohort and five-factor personality—and how they relate to the study. The Nature of the Study provides the methodology used. The key terms are then defined and include the predictor and criterion variables. The Assumptions, Limitations, and Delimitations sections are used to discuss the study's boundaries by identifying the range of participants, excluded participants, and possible limitations. The Significance of the Study should demonstrate the need for further research in the specified area. The Summary and Transition concludes Chapter 1 before focusing on Chapter 2 where the literature review focuses on the proposed areas.

Background

Information and communication technology continuously evolve with exposure to vulnerabilities in the form of sophisticated and malicious cyberattacks and other security risks (Li et al., 2019; Maddison, 2018; Tick, 2018). The rapidly growing problem associated with cybersecurity requires a balanced exploration of how individual differences such as personality and generational cohorts can impact cybersecurity

vulnerabilities (Jiang et al., 2016). The concern is that human beings are the link through social engineering that changes the security posture of systems. Shappie et al. (2019) focused on conscientiousness as a predictor of cybersecurity behavior in terms of if the individual is security-aware. Shappie et al. (2019) examined the relationship between personality as measured by the five-factor model and individual cyber-security behavior. Among the measures of behavior was a measure of individual security awareness. The study found that conscientiousness and openness predicted security awareness. Specifically, Jiang et al. (2016), Marangione (2019), and Viega (2018) all found that for the three generations studied regarding online safety, effective training is lacking but necessary to change the culture. The focus on online security and vulnerabilities has been on the general population and few have focused on generation-specific tendencies (Jiang et al., 2016).

There are four distinct generational cohorts—silent, baby boomers, Generation X, and millennial generations—that occupy the workplace (Cekada, 2012; Houck, 2011). Dimock (2018) described generations as silent or traditionalists (born 1928–1945, age-range 74–91), Baby Boomers (1946–1964, age-range 55-73), Generation X (1965–1980, age-range 39–54), and Generation Y or millennials (1981–1996, age-range 22–38). Examination of the differences that each generation possesses will help industry better understand and manage policy, training, and awareness for generational cohorts.

The Pew report concluded that millennials and Generation Z tend to view privacy differently than other generations (Marangione, 2019). The Pew Research Center conducted a study that indicated millennials overall have a lower level of trust and

detachment in areas of employers, government, and marriage (Marangione, 2019). Pereira et al. (2017) showed that privacy and security in electronic information are accessible and different levels of concern, based on generations. Marangione (2019) discussed the history of insider threats and the prevalence with millennials and their leaking classified information that leads to information security awareness. With millennials being at the forefront of classified information leaks, it is more important to understand how millennials view the definition of traitor, leaker, transparency, and treason. More important is the question of what personality trait being most prevalent in millennials than other generations.

A gap in the literature exists in the connection between personality traits, generational cohorts, and information security awareness (Pereira et al., 2017; Quan-Haase et al., 2018; Thompson et al., 2017). Complicating this gap, Cram and Proudfoot (2019) stated that studies seeking to understand the effect of critical antecedents to cybersecurity compliance such as attitudes, perceptions, personal norms, and ethics but find challenges in finding research literature. These are hampered by competing for theoretical perspectives and inconsistencies that form a theoretical stalemate and deter consensus building in different contexts.

Problem Statement

Technology enhancements are in a state of a continuous evolution and they are deployed as easy-to-manage data and systems by firms to conduct business operations and comply with regulatory requirements. In 2021, a worldwide survey accomplished by

Grant Thornton Advising indicated the United States and other countries encountered over 100,000 server compromises by malicious cyberattacks.

The importance of the social component, the human element of this sociotechnical issue, ranks as one of cybersecurity's most essential items (Cunningham et al., 2018; Kim et al., 2017; Zimmermann & Renaud, 2019) with human error or behavior representing the source of at least 90% of cyberattacks (Carlton et al., 2019). Studies confirm the social component as the weakest link in cybersecurity (Malatji et al., 2020; Zimmermann & Renaud, 2019). The specific problem is human beings are the link to the growing issues with information security. There are gaps in research that focus on the relationship between information security awareness and multiple generational workforce and if personality traits can be attributed to information security breaches.

Purpose

The purpose of this quantitative study is to assess the relationship between personality traits, generational cohort, and information security awareness. The predictor variables were (a) personality traits (openness, contentiousness, extroversion, agreeableness, neuroticism) and (b) generational cohort. The criterion variable was information security awareness. The aim was to understand information security awareness in a diverse, multigenerational workforce and their associated personality traits. Inspired by the rapidly growing problem associated with cybersecurity, the purpose was to add to the industrial/organizational literature examining the impact on information security in the professional workplaces arising from personality traits in the working generations.

Research Question and Hypotheses

In order to understand the relationship between generational cohorts, personality traits, and information security awareness, the intent of the research was to answer the following questions:

Research Question 1: What is the relationship between personality and information security awareness?

Hypotheses:

H_{A1}: A statistically significant relationship between openness and information security awareness does exist.

H_{01}: A statistically significant relationship between openness and information security awareness does not exist.

H_{A2}: A statistically significant relationship between conscientiousness and information security awareness does exist.

H_{02}: A statistically significant relationship between conscientiousness and information security awareness does not exist.

H_{A3}: A statistically significant relationship between extraversion and information security awareness does exist.

H_{03}: A statistically significant relationship between extraversion and information security awareness does not exist.

H_{A4}: A statistically significant relationship between agreeableness and information security awareness does exist.

H_{04}: A statistically significant relationship between agreeableness and information

security awareness does not exist.

H_{A5}: A statistically significant relationship between neuroticism and information security awareness does exist.

H_{05}: A statistically significant relationship between neuroticism and information security awareness does not exist.

Research Question 2: What is the relationship between generational cohort, measured as a categorical variable, and information security awareness.

Hypotheses:

H_A: Generational cohort, measured as a categorical variable, is statistically related to information security awareness.

H_0: Generational cohort, measured as a categorical variable, is not statistically related to information security awareness.

Research Question 3: Does generational cohort, measured as a categorical variable, moderate the relationship between personality and security awareness?

Hypotheses:

H_{A1}: Generational cohort does moderate the relationship between openness and information security awareness.

H_{01}: Generational cohort does not moderate the relationship between openness and information security awareness.

H_{A2}: Generational cohort does moderate the relationship between conscientiousness and information security awareness.

H_{02}: Generational cohort does not moderate the relationship between

conscientiousness and information security awareness.

H_{A3}: Generational cohort does moderate the relationship between extraversion and information security awareness.

H_{03}: Generational cohort does not moderate the relationship between extraversion and information security awareness.

H_{A4}: Generational cohort does moderate the relationship between agreeableness and information security awareness.

H_{04}: Generational cohort does not moderate the relationship between agreeableness and information security awareness.

H_{A5}: Generational cohort does moderate the relationship between neuroticism and information security awareness.

H_{05}: Generational cohort does not moderate the relationship between neuroticism and information security awareness.

Conceptual Framework

This study was grounded in two theories. First, was personality theory, and specifically the five-factor model of personality (McCrae & John, 1992). The second was generational cohort theory (Mannheim, 1972). The five-factor model of personality will serve as the conceptual framework for this study. It is a model used to measure personality in psychology (Costa & McCrae, 2008). Developed by Goldberg, the Big Five Inventory (BFI) has been used to measure the five personality factors (McCrae & John, 1992). It encompasses a portion of personality terms that are factors used to describe traits and characteristics. The five-factor model of personality was based upon

the premise that people exhibit their character at some level (Shappie et al., 2019). The five-factor approach includes characteristics described as openness, conscientiousness, extraversion, agreeableness, and neuroticism.

McCrae and John (1992) described each broad factor encompassed by more specific features measured on an upper and lower scale. The five-factor model integrates the personality constructs and assists with multiple variations of its use. Further, it offers the exploration of personality, other phenomena, and describes with a minimum of five scores developed. The five-factor model has been used in counseling, forensic, education, and health psychology.

Park et al. (2020) utilized the five-factor model to measure motivation and job performance. The use of the broad five-factor constructs included multiple narrower aspects and facets of personality. Shappie et al. (2019) utilized personality factors to predict behavior concerning security behavior, noting conscientiousness as a strong predictor. This study's findings supported a link between the five-factor model and security behavior by reviewing the knowledge level of how to behave.

Nature of the Study

The nature of this study was quantitative with the opportunity to understand the relationship between variables (Burkholder et al., 2016). Multiple linear regression analysis of five personality factors and information security awareness associated with participants found in the silent generation, born between 1928 and 1945; baby boomers, born between 1946 and 1964; Generation X, born between 1965 and 1980; and Generation Y, born between 1981 and 1996. Utilization specific to these generational

cohorts that are employed and use information and communication technology in their workplaces use objective measures of personality traits, generational membership, information security awareness, and reporting procedures specific to their profession and industry.

Definition of Key Terms

This section consists of the definitions of key terminology used in this study.

Generational cohort: Generational cohort was a group of individuals in a specific age group, living in a similar location, and experiences a significant event, living in a certain geographic location, and also having common experiences in a historical and social nature (Pilcher, 1994).

Generations

The generational cohorts relevant to this dissertation are defined as follows:

Baby boomer: The baby boomers were born between 1946 to 1964, ranging from 55 to 73 years old (Dimock, 2018). These individuals prefer simplicity, being in control, and have a quest for self-gratification (McIntosh-Elkins et al., 2007). They tend to be independent, prefer controlling their destiny and challenge authority and also have a sense of entitlement and expectation of rewards. They promote teamwork, optimism, ambition, and diligence.

Generation X: Generation Xers were born between 1965 to 1980, ranging from 39 to 54 years old (Dimock, 2018). This group was raised during the information and technology revolution that affected the communication, education, entertainment, and

home living (McIntosh-Elkins et al., 2007). Generation X flourished in diversity but traditions diminished.

Generation Y (*millennials*): Millennials were born between 1981 to 1996, ranging from 22 to 38 years old (Dimock, 2018). These individuals are a product of the baby boomer generation, and around the time of cellular mobile phone system (McIntosh-Elkins et al., 2007). Generation Y is dependent on accessible information at all times, and they experienced terrorism that shaped their perspective.

Silent/traditionalist: The silent or traditionalist generation were born between 1928 to 1945, ranging from 74 to 91 years old (Dimock, 2018). This generation born prior to World War II are considered dedicated workers and are currently holding leadership positions in the workforce (McIntosh-Elkins et al., 2007). They tend to be loyal, practical, diligent and compliant.

Personality Traits

The five-factor model was assessed by using the Revised NEO Personality Inventory (NEO PI-R) Costa and McCrae (2008), measuring the five broad domains. McCrae and Costa (1991) posited personality traits as being a set of characteristics that underlie a person's affect, cognition and behavior. Big Five or Five-Factor Model include the five broad traits: agreeableness, conscientiousness, extraversion, openness, and neuroticism. The five-factor model measures are defined as follows:

Agreeableness: An individual that exhibits agreeableness was courteous, flexible, trust and tender-mindedness (Shappie et al., 2019). Agreeableness was associated with stronger cybersecurity practices from the five personality constructs. Bakker et al. (2006)

described agreeableness as an individual that is sympathetic to others and willing to help. They are altruism, nurturance and caring individuals.

Conscientiousness: An individual that exhibits conscientiousness is impulsive control behaviors with focus on completing a task or goal, being able to accomplish task such as planning, and organizing (Shappie et al., 2019). Another trait that is associated with self-reported behaviors and a strong predictor of cybersecurity behaviors. Bakker et al. (2006) described conscientiousness individuals as those that have problem-solving, self-discipline, dutiful, reliable and competent traits.

Extraversion: An individual that exhibits extraversion is sociability and positive affectivity (Shappie et al., 2019). Extraverts are sensitive to rewards in the workplace and in association with status found throughout their lifespan. Bakker et al. (2006) characterized extraversion individuals as those that have confidence, positive emotions, talkative, sociable, excitement seeking, assertive, and intense personalities.

Openness: An individual that exhibits openness is imaginative, curious, and original thoughts (Shappie et al., 2019). Openness is associated with self-reported behaviors and security attitudes. Individuals that have an active imagination, curious, attuned to their inner feelings, and prefer variety (Bakker et al., 2006)

Neuroticism: An individual that exhibits neuroticism has feelings such as anxiety and sadness (Shappie et al., 2019). Notability found to be a negative association with self-efficacy. Bakker et al. (2006) described neuroticism as those individuals that have low self-esteem, social anxiety, poor inhibition, and helpless and experience negative emotions.

Assumptions, Limitations, and Delimitations

Assumptions

Interpretation of facts considered true without verification were assumptions that lack proof of validity. Waldkirchch (2020) recommended clearly stating and evaluating assumption, and to consider the value it contributes and determine practicality. The first assumption in this study was the ability to obtain participation of members from each generation representation for survey implementation. The second assumption was that the participants would not be reluctant to identify their responses in the research correctly. The last assumption was the ability to obtain a useful sample of each identified population.

Limitations

Potential weaknesses of the study that are beyond the control of researcher's capacity to affect the analysis of the study findings are referred to as limitations (Brutus et al., 2013). There are two limitations to the study. The first limitation was the availability of the survey to anyone under the age of 22. The purpose of limiting the age group was to ensure professional workers in the industry of technology is captured. The second limitation was the availability of participants in each age group, possibly requiring seeking other candidates from other organizations.

Delimitations

Podsakoff et al. (2012) referred to delimitations as the limits imposed by the researcher in a study by creating boundaries or scope on a study. The study participants

are in a specific geographic location. Federal workers who work within metropolitan area was a delimitation because they do not encompass all federal workers.

Significance of the Study

Existing literature has demonstrated the relationship between cybersecurity issues and information security awareness (Ifinedo, 2012; Leuprecht et al., 2016; Thompson et al., 2017). There was also existing literature demonstrating the relationship between cybersecurity issues and personality traits (Marangione, 2019; Shappie et al., 2019). This study was unique because it addresses an under researched area, the gap in the literature, articulated by Thompson et al. (2017), regarding personality traits in the working generations and how these personalities impact information security. The research results may inform generational security behavior in the work environment, testing the five personality traits and information security awareness found in each generation. This study may encourage social change by improving knowledge and creating a strategy to foster protective measures against cyber terrorists.

Positive social change from this study is that it increases the potential to raise awareness of the prominent vulnerabilities in generations by understanding interactions, use of information, and business dealings. The impact on social change can further affect policy, provide protection personally, and corporations nationally.

Summary and Transition

The purpose of this quantitative study was to assess the relationship between personality traits, generational cohort, and information security awareness. To accomplish this aim, the study was used to consider information that can answer what the

relationship exists between personality, generational cohort, and information security awareness. I also examined whether generational cohort moderated the relationship between personality and security awareness. The survey design was quantitative survey with a convenience sample of federal workers. Gaining an understanding of multiple generations in the workforce can help individuals and organizations to identify generation-specific styles to improve information security awareness.

Chapter 2 provides a critical review of the synthesized literature about the formation of generational cohorts and the ways in which they differ on different levels. After a discussion of the basics of generational cohort theory and its uses in the workplace, the focus turns to the five personality traits and how each trait influenced the generational cohort as measured against information security awareness. Information security awareness is reviewed focusing on the means of malicious attacks and security risks. The review concludes with a discussion of generational differences in the workforce and the need for additional research. The purpose of the literature review was to increase the current knowledge base, as well as to identify gaps. The study methodology is described in Chapter 3, and Chapter 4 contains a discussion of the presentation of the results. Lastly, Chapter 5 contains the conclusions and recommendations for future research.

Chapter 2: Literature Review

This literature review explored theories relating to personality, generational cohorts, and information security. The rationale for choosing the five-factor model for assessing personality constructs for workers' information security measures will be discussed. The use of Mannheim's generational theory is also considered. This chapter includes an introduction that provides an in-depth discussion of generational cohort theory, personality traits and information security awareness. Next, the Literature Search Strategy describes the extensive search and criteria used to find pertinent literature. The remainder of Chapter 2 includes a description of the theoretical foundation and literature review related to key terms and concepts. Finally, the Summary and Transition section will summarize the themes found in the literature review.

Though research exists on generational cohorts (Mannheim, 1952), personality traits (Costa & McCrae, 2008; Shappie et al., 2019), and cybersecurity awareness (McCormac et al., 2017), there is limited research that examines the three together and the impact in security structures. By examining generations and personality traits, the expectation was to provide a better understanding of their impact on information security awareness.

The five-factor model provides an approach to comprehend personality (Goldberg, 1993). The terms used in the five-factor model provide a means for individuals to describe themselves (John & Srivastava, 1999). The five-factor model, also called Big Five personality, has been utilized in examination of cybersecurity behavior in previous research, resulting in no apparent consensus on which factor was critical

(Shappie et al., 2019). However, Shappie et al. (2019) suggested that the personality traits associated with security behavior were conscientiousness and openness. Yet, authors McCrae and Costa (1991) and Shropshire et al. (2006) suggested intention as a predictor of cybersecurity behavior. McCrae and Costa also pointed out that attitudes and personal strivings moderate the connection of personality constructs and behavior.

Organizations spend time and resources to secure their cyber systems, only to have them circumvented by individuals. However, organizations can minimize vulnerabilities by increased vigilance and desktop security programs that target high-risk users, and these measures can be cost-prohibitive (Shropshire et al., 2006). Sources have suggested their threat is not external but the careless actions of individuals in the organization that practice non-compliant security behavior (Shropshire et al., 2006). Most information security violations are due to negligence or ignorance (Lee et al., 2016).

Information security awareness was a prominent discussion for businesses and government entities (Li et al., 2019). Cyberattacks are becoming more sophisticated and complex creating greater security risks in society (Li et al., 2019). Researchers (Carlton et al., 2019; Li et al., 2019) have studied cybersecurity attacks relating to workplace behavior. Carlton et al. (2019) found that individuals with increased age, experience, education level, and the use of information technology showed an improvement in reducing unauthorized leakage. This review addressed how personality traits influence information security awareness within the multiple-generation workforce. Creating an understanding of how each generation tends to behave makes it possible to examine the workforce's influence on security.

Research shows that users' poor cybersecurity skills result in 95% of mistakes in cyber threats for organizations (Carlton et al., 2019). As technology and internet access has increased easily managed data and systems for businesses and individuals, systems are more susceptible to malicious cyberattacks and security risks (Thompson et al., 2017). Jiang et al. (2016) discussed the susceptibility of online security threats for three generations—the silent generation, baby boomers, and millennials—focusing on the perceived safety and protection. Additionally, vulnerabilities from sophisticated and malicious cyberattacks and other security risks continue to evolve and expose information security risks (Li et al., 2019; Maddison, 2018; Tick, 2018).

Preliminary research findings suggested a vital source of organizational risk of hacking, either accidental or aided by workers who possess little understanding of technology or its implications (Cunningham et al., 2018; Thompson et al., 2017). Other research suggested personality may predict the cybersecurity behavior of a user's best intentions by maintaining compliance with policies, the risk to data, and safety measures (Shappie et al., 2019). Because society has become more dependent on technology, threats impact the greater population. Shappie et al. (2019) found linkages to the Big Five by self-reporting cybersecurity behaviors. Their research suggested that personality structure was associated with behaviors found in cybersecurity showing that conscientiousness and openness are important to the relationship. This study investigates the association between personality traits and cybersecurity behaviors.

The introductions of digitized instrumentation and controls systems have increased the cyber threats in nuclear power plants (Kim et al., 2017). The study

presented by Kim et al. (2017) focused on human actions that affect the safety of systems. Their study utilized the fault tree model to assess the system error found in cybersecurity issues using the human error probability citing a conditional probability for a successful hacker attack.

Intention was considered a cognitive process that has been the focus of previous research and used as a predictor of cybersecurity behavior (Shropshire et al., 2015). The Big Five personality traits that influence security attitudes, intentions, and behavior are conscientiousness and agreeableness in their ability to moderate the relationship (Shropshire et al., 2015). As those two traits increased, the relationship between intention and initial adherence to the security practice also increased (Shappie et al., 2019; Shropshire et al., 2015).

Literature Search Strategy

The literature search strategy was to collect all information that is discussed in this chapter, and conduct an extensive review of the research literature in multiple areas. Use of the Walden University Library academic databases included Google Scholar, ProQuest, and Sage Publications. The databases searched were Thoreau Multi-Database; Psychology, Counseling, Information Systems and Technology; PsycARTICLES; PsycINFO; and Academic Search Premier.

There are multiple approaches to the literature review: argumentative, integrative, methodological, systematic, narrative, and theoretical reviews (Banomyong et al., 2019). Utilizing an iterative review process allows a comprehensive search for literature that

enables integration of quantitative data, and theoretical framework, and understanding the topic (Boyle et al., 2018; Snyder, 2019).

This review of academic and professional literature included a comprehensive search of articles related to generations, Big-Five, and information security awareness. The primary search terms used were as follows: *generational cohort theory, generations, silent or traditionalist generation, baby boomers, Generation X, Generation Y, millennials, information security, cybersecurity, Human Aspects of Information Security Questionnaire (HAIS-Q), security behaviors, self-efficacy, perceived barriers, questionnaire designs, cyber terrorism, Big five personality, humans role problematization, socio-technical system, behavioral information security, home computer security, induced human error, no- safety system, social engineering, cyber-crime, intrusion detection, Five-Factor Model of personality,* and *personality traits.*

Theoretical Framework

The theoretical framework for this study was based upon generational cohort theory and five-factor model of personality (Mannheim, 1972). Generational cohort theory has been studied by many; however, Karl Mannheim published an essay in 1923, *The Problem of Generations,* which originally was to understand, categorize, and define generational cohorts (Mannheim, 1952). Several studies utilized Mannheim's cohort theory and alternate uses to this method offered in research. Much of the work following Mannheim was influenced contemporary work (Connolly, 2019). Howe and Strauss (1991) used the generational cohort theory to show the differences in individuals' values, their motivations, and beliefs being the result of events that occurred during a certain

timeframe. And the uses for trait theory have made progress and provided strong empirical support for studies and organized by five traits (Fleeson & Jayawickreme, 2015). The five-factor model is defined by Costa and McCrae (2008) as a tool that measures personality using five domains: openness, conscientiousness, extraversion, agreeableness, and neuroticism. McCrae and John (1992) described each broad factor encompassed by more specific features measured on an upper and lower scale. The five-factor model integrates the personality constructs and assists with multiple variations of its use (McCrae & John, 1992). Further, this model offers the exploration of personality, other phenomena and describes with a minimum of five scores developed (McCrae & John, 1992).

Generational Cohort Theory

Howe and Strauss (1991) used the generational cohort theory to show the differences in individual's values, their motivations, and beliefs being the result of events that occurred during a certain timeframe. For example, Popescu (2019) presented work that considers a link between social systems and family systems. The family system is considered the family tree and the social system is considered a group of people of the same age and share cultural characteristics (Popescu, 2019). Turner (2002) examined the lag in social effects from traumatic events and the emergence of generations past and future. The results from studies presented by Turner was that social change could be the direct outcome of actions specific to that generation. Research presented by Cogin (2012) reviewed four generations in the workforce that suggested difference in expectations and motivation across the cohorts. Cogin found significant differences in Generation Y,

showing a decline in work ethic. Generation X and Y showed they have less sense of pride in their work compared to other generations (Cogin, 2012).

Generation is a term which has multiple meanings and is used to describe various categories of factors: the age group, a time frame, theory to the kinship, and generation of a historical regnum (Mannheim, 1952; Popescu, 2019). Generation is used daily to describe human beings and with multiple defined delineations of a population. The use of the term *cohort* defines a group of individuals that are born in the same timeframe and have similar experiences (Rogler, 2002). Edmunds and Turner (2005) defined *generational cohort* as individuals who were born in about the same timeframe and experience events in history about the same time in their development. Howe and Strauss (1991) categorized the cohort group by four groups: silent generation, baby boomers, Generation X, and millennials or Generation Y. During the review of the literature from multiple researchers, the definition of generational cohorts varied slightly in defined age ranges. However, they had similarly defined characteristics. Social phenomenon generation is the description that represents an identity of location, a relation to age groups in a historical-social process (Mannheim, 1952).

Generational cohort theory, used by multiple researchers, describes a group or groups of individuals born within a similar period, a social construction influenced by historical and social contexts. Mannheim's generational cohort theory has been used by researchers to describe differences in attitudes and behavior. Mannheim's generational cohort theory is used by marketers and academics to market to specific cohorts based on the attitudes, ideas, values, and beliefs.

The generational diversity in the workplace brings differing values and work ethics (McIntosh-Elkins et al., 2007). This mix of generations creates multiple challenges because of the diversity among them. Additional issues have arisen with ideas of working and ethics in each generation. The characteristics of these generations shape their role in the workplace and help us understand their experiences (McIntosh-Elkins et al., 2007).

The current workforce contains four of the generations working together. There has been research conducted to understand how these cohorts work together and how leadership can assist with bringing them together to accomplish a common goal. Sessa et al. (2007) studied the leader's role in generational cohorts, citing differences in value attributes in leaders and behavior difference. Research conducted by Salvosa and Hechanova (2020) on leadership of generational cohorts suggested that there is not a one-size-fits-all approach to leading these groups of workers. The generations have differing ideas of values and motivation (Salvosa & Hechanova, 2020).

Silent Generation, Baby Boomers, Generation X, & Millennials

At present, there are four generations in the workforce, all dealing with cybersecurity from different perspectives. An exploration of the background of each generation of people provide consideration of the individuals security awareness. The goal was to have a better understanding of the four generations. Each of the generations are briefly described next.

Silent Generation (1928–1945)

Individuals in this generational category were born after the Great Depression and up to World War II. Some are still in the workforce and they dress in a more professional

manner. The silent generation were able to separate the work and family life and were conformist (Verschoor, 2013). The silent generation were considered loyal, disciplined, and knowledgeable in work ethics (Cekada, 2012). Because of their loyalty, they tended to trust their leaders, and they were able to form work groups that worked towards common goals that benefited the community (Cekada, 2012). The silent generation are not accustomed to the technology advances, tend to adapt to change slowly, and may be generally overcautious (Cekada, 2012).

Baby Boomers (1946–1964)

Baby boomers, on the whole, are individuals who value simplicity and control, also known as the "me" generation based on their desire for self-gratification (McIntosh-Elkins et al., 2007). Baby boomers were on the leading edge of the Civil Rights movements, and are now in positions of power that enable them effect change (McIntosh-Elkins et al., 2007). The typical family of this generation included a stay-at-home mother in the suburbs and hard-working work ethics with the idea of doing their time in the workplace (Cekada, 2012; McIntosh-Elkins et al., 2007).

During the baby boomer era, medical discoveries were advancing and humans walked on the moon. Also, during this timeframe, development of technology such as radios and televisions occurred and became common. The baby boomers were the leaders in development of industry and had the larger financial effect on the economy (McIntosh-Elkins et al., 2007; Simons, 2010). The baby boomers also experienced a recession that hindered their retirement plans, thus prompting them to delay their retirement and take management positions in the workplace.

Generation X (1965–1980)

Generation X are the individuals who were born between 1963 and 1980. Generation X were the post-baby-boomer generation during the advertising industry and information technology. The information and technology era were the beginning of change for entertainment, communications, home life, and education. This generation is sometimes referred as the "latch key" children. This group had either both parents that worked or in some cases divorced, and they were raised to be independent and self-reliant. These individuals account for approximately 34% of the workforce.

During this era there was more mistrust of what was known to the baby boomers and silent generation for traditional values and the doing things the same way (McIntosh-Elkins et al., 2007). This generation questioned many things that were considered normal, exploration was welcomed, and they flourished in a dynamic environment. During this timeframe, it was more prevalent to see Generation X being raised in single-parent household and adualts saw no issue with co-habitation without marriage in their generation (McIntosh-Elkins et al., 2007). They tend to view life with flexibility, be able to manage the daily decision making, prefer variety in the workplace, and have an entrepreneurial attitude.

Millennials or Generation Y (1981–1996)

Millennials are also known as Generation Y, Gen Y, Millies, and the Entitled Generation, to name a few. This generation tends to be low risk in terms of behavior and are drawn to large corporations for employment (Howe & Strauss, 2007). They are more

transient where employment is concerned and less loyal than the silent generation. Millennials prefer immediate feedback and recognition from their bosses.

During this era, a large percentage of individuals used television as entertainment. This generation is typically less interested in reading instructions, love to experiment with technology, but adapt well with information management and instant communication technologies (McIntosh-Elkins et al., 2007). This generation also grew up when the World Trade Center was attacked. Some in this generation tend to feel entitled and could have unrealistic expectations in how they should progress in the workforce.

The four generations may differ in terms of how they are distributed on the continua of the five personality traits. The silent generation tend to thrive on spontaneity, are open-minded, and like to explore new places which describes the openness trait. Conscientiousness is more prominent in older generations in terms of self-monitoring (Whitty et al., 2015), whereas extraversion is more prominent in younger generations where they are stimulated by of social interaction (Kersting, 2003). Individuals who are easy to like or get along with, have good-natured personalities, and are approachable are found among Generation X, baby boomers, and the silent generation, which falls in line with the agreeableness trait (Kersting, 2003). Neuroticism is found mostly in the three older generations (i.e., silent, baby boomers, and Generation X) and not the two younger generations (i.e., Generation Y and Z) and encompasses the ability to withstand stress, remain even-tempered, and not allow negativity to bring them down (Kersting, 2003).

Five-Factor Model of Personality

The Big Five personality model has been used to measure personality in the area of psychology (Costa & McCrae, 2008) and will serve as the theoretical framework for the personality component of this study. It encompasses a portion of personality terms that are factors used to describe traits and characteristics. The five-factor approach includes characteristics described as openness, conscientiousness, extraversion, agreeableness, and neuroticism. McCrae and John (1992) describe each broad factor encompassed by more specific features measured on an upper and lower scale. The five-factor model integrates the personality constructs and assists with multiple variations of its use (McCrae & John, 1992). Further, it offers the exploration of personality, other phenomena and describes with a minimum of five scores developed (McCrae & John, 1992).

The five-factor model has varying uses. For example, Shropshire et al. (2006) conducted research using the personality traits to measure security compliance for individuals. Resulting research by Shropshire et al. showed conscientiousness and agreeableness had a significant relationship to security compliance. Another example is Bakker et al. (2006) conducting research using the personality traits to measure burnout. By utilizing multiple regression analysis Bakker et al. (2006) were able to show that personality may help protect against risks for volunteer counselors.

Shappie et al. (2019) and Shropshire et al. (2006) specifically focus their research in the area of information security and personality traits. Shappie et al. conducted research to predict the cybersecurity behavior in relations to a person's intention. The use

of linear regression found that personality plays a role in understanding behaviors by siting conscientiousness, agreeableness, and openness were significantly associated with cybersecurity behaviors by self-reporting (Shappie et al., 2019). Studies found there is a link between cybersecurity behavior and personality traits.

The five-factor model is a valuable tool in counseling (McCrae & Costa, 1991), forensic (Becerra-García et al., 2013), education (Göncz, 2017), and health (McCrae & John, 1992; Sutin & Terracciano, 2016) psychology. The NEO Personality Inventory (NEO-PI) is a measurement of the five-factor model utilized in counseling based upon its non-psychopathological content, sensitivity to the client's weaknesses and strengths, and shorter length shorter-term counseling (McCrae & Costa, 1991). In counseling, personality inventories and the five-factor model are helpful in measuring characteristics that exhibit more relevance than sex or age factors. The NEO-PI is not a tool to render diagnosis but instead measures traits related to anxiety, depression, and hostility (McCrae & Costa, 1991).

The use of the five-factor model in forensic psychology allowed Becerra-García et al. (2013) to capture the relation of offenders and traits correlated to childhood history. The five-factor model is used in forensic psychology to study a felon's behavior in areas such as offending, antisocial behavior, aggression, and violence, where neuroticism is high in association with violence, theft, and vandalism (Becerra-García et al., 2013). In many cases, offenders had some history of childhood trauma, physical or emotional abuse contributing to their personality.

In one study of teachers in the classroom, education psychology found extraversion limitations for producing thoughts and feelings that bring change and challenges in the class environment (Göncz, 2017). Neuroticism can show repression signs to avoid negative information but exhibit good healthy behaviors under their control (Göncz, 2017). The five-factor model's essential traits- conscientiousness, extraversion, agreeableness, and neuroticism, were utilized in education psychology. These traits measure the correlation between job satisfaction and four of the five characteristics.

Health psychology uses the five-factor model to measure personality traits and body weight in adults. Negative emotions found in neuroticism and higher conscientiousness for lower body mass indexes (Sutin & Terracciano, 2016). The research conducted by Sutin and Terracciano (2016) showed that personality linked subjective and objective obesity in young adults.

Park et al. (2020) utilized the five-factor model to measure motivation and job performance. The use of the broad five-factor constructs included multiple narrower aspects and facets of personality. Shappie et al. (2019) utilized personality factors to predict behavior concerning security behavior, noting conscientiousness as a strong predictor. Shappie et al.'s findings supported a link between the five-factor model and security behavior by measuring individuals' knowledge level. On the other hand, Shropshire et al. (2006) utilized the model to understand and predict factors in the environment that are diverse and complex. Shropshire et al. proposed that individuals demonstrate security compliant behavior and patterns. For instance, Costa and McCrae (2008) utilized the personality test to review the common individual differences in

personality. Each was using self-reported questionnaires to evaluate Neuroticism, Extraversion, Openness, Conscientiousness, and Agreeableness. The Neuroticism, Extraversion, and Openness Personal Inventory (NEO-PI) have been used in clinical settings and research to measure clients' personality and treatment variables.

Individuals exhibit dimensions of personality and have differences among them. The five-factor model can organize the traits into a coherent manner in research to show a relationship (McCrae & Costa, 1991). The model consists of the following traits: agreeableness, conscientiousness, extraversion, neuroticism, openness.

Agreeableness

A trait found in the five-factor model is an aspect of interpersonal behavior where individuals are trusting, sympathetic, cooperative, cynical, callous, and antagonistic (Costa & McCrae, 2008). Characterized by a willingness to help other people and sympathetic. This dimension also describes how a person interacts with others and a collection between compassion to antagonism (Becerra-García et al., 2013). The agreeableness trait has characteristics of caring and one that provides emotional support, but the opposite end of the spectrum includes hostility, self-centeredness, and jealousy (McCrae & John, 1992).

Conscientiousness

A trait found in the five-factor model that exhibits impulsive control behaviors geared toward completing goals or task completion, often found with planning, organizing, and delaying gratification (Costa & McCrae, 2008). Conscientiousness is characterized by problem-solving, self-discipline, dutiful, reliable, and competent. The

degree of organization, control, and persistence found in a person directed by conscientiousness (Becerra-García et al., 2013).

Extraversion

A trait found in the five-factor model that exhibits sociability experiences positive emotions such as joy and pleasure (Costa & McCrae, 2008). Extraversion can be characterized by self-confidence positive, assertive, sociable, and talkative. Extraversion reflects the amount and intensity of positive interactions found between people, the need for stimulation, and the indication of sociability found in joy and to seek stimulation from outside sources (Becerra-García et al., 2013). Extraversion is defined by dominance and affiliation (McCrae & John, 1992). Low functioning extraverts are quiet, shy, and withdrawn, seeming more like introverts (McCrae & John, 1992).

Neuroticism

A trait that contrasts emotional stability and exhibits feelings like anxiety and sadness (Costa & McCrae, 2008). Characterized by their fearful nature, low self-esteem, and helplessness. Neuroticism reflects a person's emotional adjustment and predisposition of an experience affect (Becerra-García et al., 2013). High-scoring neuroticism tends to experience adverse effects and prone to a variety of psychiatric disorders (McCrae & John, 1992). The opposite neuroticism found in low scores tends to be calm, relaxed, even-tempered, or unflappable (McCrae & John, 1992).

Openness

A trait that exhibits an extent where an individual's mind and experiences are complex and original (Costa & McCrae, 2008). Characterized by one with an active

imagination and curious nature. Openness is the aesthetic sensibilities, searching for new experiences, and using one's imagination (Becerra-García et al., 2013). Openness describes more of a personality trait, interest levels, creativity, curiosity, and artistic (McCrae & John, 1992). Lower-end openness holds conservative values and has aspects of intellect in a broad scope (McCrae & John, 1992).

Information Security Awareness

Dependency on information systems has required additional measures to mitigate the information security threats being introduced. An initial review of literature for this study showed that previous work has been accomplished to examine information security awareness and the knowledge of policies and procedures among employees (McCormac et al., 2017). McCormac et al. (2017) contends that age is a component that does not explain differences in information security awareness. Information systems are threatened daily by the carelessness or maliciousness of individuals using those resources (Pfleeger & Caputo, 2012; Thompson et al., 2017; Warkentin & Willison, 2009; Willison & Warkentin, 2013). Other research supports information and communication technology continuously evolves with exposure to vulnerabilities in the form of sophisticated and malicious cyberattacks and other security risks than ever before (Li et al., 2019; Maddison, 2018; Tick, 2018).

Information security awareness considers if the users are aware and committed to the organizations mission regarding security. The characteristics of information security awareness contains two aspects, understanding the importance of information security policies or guidelines, and the commitment to following best practices found in policies

and guidelines. Parsons et al. (2014) developed the Human Aspects of Information Security Questionnaire (HAIS-Q) to focus on seven areas: internet use, email use, social networking site use, password management (including locking workstations), incident reporting, information handling and mobile computing (Jiang et al., 2016; Li et al., 2019; Parsons et al., 2014).

One human behavior that is part of the seven areas, password management, is inadvertent or deliberate, putting the organization at risk (Jiang et al., 2016; Li et al., 2019; Parsons et al., 2014). Part of password management includes creating a strong password that is harder to hack for accounts. Next, email use includes opening attachments, forwarding emails, and opening emails from unsolicited or unknown sources, creating vulnerabilities in the IT structure, and refusing to engage or open them reduces the susceptibility of breaches (Jiang et al., 2016; Li et al., 2019; Parsons et al., 2014).

Information security awareness continues to be a vulnerability for users and organizations. Sheehan et al. (2019) defined weaknesses in a system as vulnerabilities that can be exploited and the cause of adverse outcomes. Information security awareness is defined as the level of awareness or understanding of importance of information system security, secure behavior, and the responsibility of the individual to maintain security of resources (Mejias & Balthazard, 2014).

Scholars have made the point of humans being the vulnerable link in the cybersecurity chain (de Bruijn & Janssen, 2017). Issues resulting in failure to create policies, not taking appropriate actions to handle cybersecurity threats. Research

indicated there is limited visibility and society neglecting appropriately reactions to threats. Consideration of communication measures that do not create misunderstanding and ambiguity is needed for effective results (de Bruijn & Janssen, 2017).

Additionally, internet use, social networking site use, and mobile computing are three additional areas that introduce cyberattacks (Jiang et al., 2016; Li et al., 2019; Parsons et al., 2014). The complexity of installing software on devices, accessing questionable websites on work and home computers, openly posting personal or work information, and using mobile devices to send or receive sensitive information increases risk (Parsons et al., 2014).

And finally, incident and information handling areas can be considered essential and controllable in the workplace or home environment. Information handling includes documents, media, and sensitive information (Parsons et al., 2014). These seven areas describe multiple means of malicious attacks exploited daily. These two areas require one to be aware to prevent incidents of mishandled information or to report the incidents immediately. These seven areas describe multiple means of malicious attacks that exploited daily, and each site viewed differently.

Summary and Transition

This research assessed the relationship between generational cohort, personality traits, and information security awareness. In this section an assessment of the generational cohort theory and personality traits was used to evaluate the impact on information security awareness and whether these items have impact on security awareness for organizations and personal security. The literature review was an

investigation to understand the predictor and criterion variables. The review shows the need for additional research and clarification of the constructs of personality traits, generational cohorts and their effect on information security awareness. Trials have been conducted by researchers using the Big five model to determine distinctions between generational cohorts in terms of personality traits and in differing research in terms of information awareness in the workplace. Multiple generational cohorts work in organizations daily and the differences are their ages, and work experience.

Several studies focus on topics concerning cybersecurity behavior and its effect on hacker's success rate (Li et al., 2019). Most research attempted to explain information security behavior in the workplace. The research presented by Li et al. (2019) found employees were more competent after they were aware of information security policies and procedures. Research presented by Parsons et al. (2014) incorporated the HAIS-Q developed scales to study various factors of employees. The review of personality trait theory showed distinct traits that were consistent over time (Costa & McCrae, 2008; Fleeson & Jayawickreme, 2015; McCrae & Costa, 1991;). It was found that the Big Five traits—openness, conscientiousness, extroversion, agreeableness, and neuroticism—were the dominant traits (Costa & McCrae, 2008; Fleeson & Jayawickreme, 2015; McCrae & Costa, 1991). The review demonstrates that generation may have an impact on security related behaviors. The review also demonstrated that personality is related to cybersecurity behaviors. However, there remains a gap to see if there in an interplay between generational cohort, personality, and cybersecurity. This study investigated these relationships.

In Chapter 3, the research method of the study is discussed with a description of the measurements, rationale, research questions and design. The chapter will include a description of the population, sampling methods, and the sample that will be taken from the population for the study. The data collection and data analyses methods, and summary of the entire chapter

Chapter 3: Research Method

In this quantitative study, I assessed the relationship between personality traits, generational cohort, and information security awareness. Information security is an issue of critical importance today and in the future. The study includes individuals who fit each generation's profile and those who work with information security. The participants required screening to ensure they fit the profile for the study. The participants had to fit within the age range of the generation cohorts of interest. I used multiple regression analysis to answer the research questions. The regression analysis determined whether the predictor variables (generational cohort and personality traits) have a statistically significant relationship with information security awareness. The research may contribute to a better understanding and impact of generational cohorts and personality and an impact to information-security awareness. Multiple regression analyses were used to answer the research questions. This chapter covers the research design and rationale, methodology, threats to validity, and summary.

Research Design and Rationale

The study was a quantitative cross-sectional survey design. The predictor variables selected for the study are generational cohort and personality traits derived from the five-factor model. The criterion variable was information security awareness. The data were collected using a self-reported survey provided to the participants. The primary purpose of the study was to evaluate whether personality traits predict a cohort's information security awareness in the workplace. The survey design assisted with answering descriptive questions about people, including questions about the relationship

between the predictor variables and questions about the predictive relationships between variables over time (Creswell & Creswell, 2018). Cross-sectional surveys provide a numeric description of key variables of interest and allow for exploring relationships among the measured variables (Creswell & Creswell, 2018). The use of surveys was economically feasible with a rapid turnaround in data collection (Creswell & Creswell, 2018).

Methodology

The methodology section describes the target population, sampling strategy procedures used to identify the study participants, sampling strategy, techniques used to draw the sample, a description of the sampling frame, the data collection procedures, and instrumentation.

Population

The target population for the study were adults employed in the technology field ranging in age from 18 to 85 years old. The survey was populated by requesting the individual take the survey to enter their age by use of a drop-down response option populated with age values as integers (e.g., 23, 24, 25, and so on). The age values can be converted to the appropriate generational cohort. Additionally, the adults had to be working with computers or information security or technology and could be members of the government, industry, and full/part-time employees. The Occupational Employment Statistics (OES) program indicates over 866,000 individuals are working at the federal, state, and local government levels in the United States. The assessment of individuals

who use information security answers the relationship to the research questions identified for the study.

Sampling and Sampling Procedures

The research used convenience sampling, which included soliciting individuals from various sources. The ideal situation was to request participants via the internet using social media sites. The survey distribution method for LinkedIn and Facebook was to use professional networking groups for voluntary participants. The solicitation occurred by requesting permission to post the survey to social media sites and providing a link to the study in their group. The approach increased geographic diversity of the sample compared to targeting a single company or the geographic area. In addition, it minimized challenges to obtaining agreement from organizations that might be apprehensive regarding autonomy and trust. In the event of difficulty acquiring potential participants, snowball sampling, a technique recruiting existing participants from their acquaintances to participate in the sample group, (Creswell & Creswell, 2018) could have been incorporated.

The best method used to determine the number of participants for the study was the incorporation of power analysis based on the statistical power, the desired alpha level, and an empirical estimate of the effect size (Bernard, 2013). The probability that a statistical test will reject the null hypothesis is called *power* (Liu et al., 2012). There were two predictor variables for the study. G*Power provides a statistical power analysis designed to analyze different types of power and compute sample size for linear multiple regression. The effect size using the G*Power statistical calculator large enough to

maintain a margin of 5% error and with a confidence level of 95%. (Faul et al., 1996). Based on the G*Power analysis, the sample size needed was 107 and was the basis of the alpha value of .05 and a medium-sized effect derived from other studies.

Data Collection Procedures

Survey data were collected online using the free online survey platform SurveyMonkey (https://www.surveymonkey.com), which has a social media collector to use on social media sites such as LinkedIn. This method allowed the creation of a link to the survey to be placed on the sites of choice. Five groups in LinkedIn were used to target participants for the survey: (a) Software and Technology Professionals; (b) Cybersecurity: Law, Policy and Technology; (c) Information and Communications Technology (ICT) & Cybersecurity; (d) Information Technology Group: Cybersecurity Professionals Network; I and Cybersecurity: The Intersection of Policy and Technology. There were additional groups to supplement the survey participants to ensure the sample size was met.

The research aligned with the Ethical Principles of the Psychologists and the conduct specified in the American Psychological Association (2002). To comply with APA guidelines, the first page of the survey showed the IRB-approved informed consent form. The informed consent form was available on the page once the participant entered into SurveyMonkey. Consent was provided by continuing forward with the survey. The survey measures were detailed in the Instrumentation section. Those who completed the survey were taken to a thank you page, created as part of the survey in SurveyMonkey, after they completed all the survey items.

Instruments

Data were collected using two measures. First, the BFI, similar to that presented by Costa and McCrae (2008) created by John and Srivastava (1999; see Appendix A) and the HAIS-Q used by Parsons et al. (2017; see Appendix A). In addition, participants completed demographic items such as age, part-time, full-time, unemployed, and gender. Each of these measures are detailed below, along with information on reliability and validity. The demographic items, they are explained along with the sources for the items.

The BFI

The BFI is a 44-item assessment designed to assess of the big five or five-factor model of personality. Neuroticism (N), extraversion (E), and openness (O) have been found to generalize across age, culture, and measurement (John & Srivastava, 1999; McCrae et al., 2011). The BFI included neuroticism, extraversion, openness, agreeableness, and conscientiousness (Costa et al., 2008; John & Srivastava, 1999). The inventory consisted of items that measured each personality domain using a 5-point Likert scale: strongly disagree (SD), disagree (d), neutral (N), agree (A), or strongly agree (SA).

The BFI is a measure in research developed in response to researchers seeking a more efficient tool (Gosling et al., 2003). The BFI is 44-item assessment tool that uses short phrases that relate to the five dimensions of personality (John & Srivastava, 1999). John and Srivastava (1999) showed a discriminate correlation of .33 for BFI. Using BFI, the average discriminant correlation for agreeableness and conscientiousness was .28. Big

five are independent dimensions that measure with convergent and discriminant validity (John & Srivastava, 1999).

Reliability. The reliability found by John and Srivastava (1999) compared to the NEO-FFI resulting in the coefficient alpha reliabilities of .83 in comparison to NEO-FFI, which resulted in .79. There has been a convergence study between the BFI and NEO Personality Inventories. The findings show a strong convergence between the BFI scale and the corresponding facet in the NEO PI-R (Soto & John, 2008).

Validity. There is extensive information found in the *NEO Inventories Professional Manual* (Costa & McCrae, 2008) for the convergent and discriminant validity of NEO-FFI. Demonstration of the convergent validity demonstrated via correlations with Goldberg's (1992) Trait Descriptive Adjective (r =.81), John and Srivastava (1999) reported 56 for the BFI, and Costa and McCrae's (2008) NEO FFI (r =.73; John & Srivastava, 1999). Researchers have reported that the studies using the BFI are easier to synthesize with other big five models.

The HAIS-Q

The HAIS-Q was used to provide a benchmark for evaluating effectiveness. The HAIS-Q was previously used in other studies, and numerous safeguards and testing were designed to ensure validation and reliability (Parsons et al., 2014). The HAIS-Q utilized a three-phased approach presented by Parsons et al. (2014). Phase 1 was the validity phase to obtain the face validity of the tool. Phase 2 included a pilot study to refine and examine the reliability. Finally, in Phase 3, the validity and reliability were used to measure a series of Pearson product-moment correlations further (Parson et al., 2014). The

researchers modified the questions to ensure the best fit and accurate measurement of constructs. The inventory consists of a 5-point Likert scale (1 = *strongly disagree* to 5 = *strongly agree*).

Reliability and Validity. The HAIS-Q has been utilized in multiple research types in quantitative and qualitative studies. The reliability of Parsons et al. (2014) ranges from .844 to .918 for Cronbach's alpha. Some studies show the reliability and validity of the HAIS-Q by using questions specific to their research (McCormac et al., 2016; McCormac et al. 2017; Parsons et al., 2017; Wiley et al., 2020). Wiley et al. (2020) reported an alpha of .69 using specific questions related to information security awareness. The internal reliability exceeded Cronbach's recommended alpha coefficient of .70 (Cronbach, 1951) for each of the seven areas found in the HAIS-Q, resulting in between .75 and .82 (Parsons et al., 2017). This indicates that items within the scales of HAIS-Q will be consistent in measuring information security awareness. In addition, Pattinson et al. (2019) also utilized the HAIS-Q survey resulting in .96 for the alpha coefficients.

Validity. The HAIS-Q of Parsons et al. (2017) presented two studies that further establish convergent validity. The convergent validity demonstrated with other theoretically related measures (Westen & Rosenthal, 2003).

Demographic Information Form

The demographic form used was the standard information for the participants which included age, gender, education level, work status, and length of employment. The items were derived from a self-report survey. Age was measured as an integer in years by

category to ascertain which generational cohort the respondent belongs to, and gender was measured by asking participants to choose between two text answers (male or female). Education level derived from categories of highest degree obtained (less than high school, high school degree or equivalent, some college, associate, bachelor, or graduate degree). Work status was measured using best-fit employment status categories (employed, working 1–39 hours/week, 40 or more hours/week, not employed, retired, disabled, unable to work) and the employment years (0–4, 5–10, 11–15, or 15 or more).

Threats to Validity

Validity deals with the steps taken to check for the accuracy and credibility of the proposed findings (Creswell & Creswell, 2018). Creswell and Creswell (2018) mentioned two potential threats to validity: internal and external threats. The internal threats to validity are the participants' procedures, treatments, or experiences. Moreover, external threats are those items that draw incorrect inferences from the data about other persons, settings, and past or future situations (Creswell & Creswell, 2018). The study pursued select participants within the specified career fields with the goal of similar results.

Threats to validity may occur because of the self-report nature of the study. Participants responded to research questions, and some chose to discontinue the study during the survey. There was a lack of complete responses, resulting in incomplete data or results gathered for the study. The incomplete data was not allowed to determine the impact for each group. If participants did not provide honest answers to the questions, there will be a direct impact on the validity of the data captured in the study.

Data Analysis Plan

The Statistical Package for the Social Sciences (SPSS, Version 28) software was used to assist with analyzing the data collected from the participants through SurveyMonkey. Demographic information was used to categorize the individuals and describe the samples received for the population of interest. The predictor variables, generational cohorts, and personality traits were assessed for the study.

The invitation I created included a letter of consent, which contained the purpose of the research and gave potential participants the opportunity to decline the invitation. Those individuals who chose to take the survey were able to select the link to the survey. The selection of the link meant the participants agreed to accept risks associated with the survey. Participants could stop taking the survey at any time. I reviewed the survey to ensure the data were usable. Any surveys that were rejected or incomplete were removed from inclusion in the research.

The study addressed the following research questions and their associated hypotheses:

Research Question 1: What is the relationship between personality and information security awareness?

H_{A1}: A statistically significant relationship between openness and information security awareness does exist.

H_{01}: A statistically significant relationship between openness and information security awareness does not exist.

H_{A2}: A statistically significant relationship between conscientiousness and information security awareness does exist.

H_{02}: A statistically significant relationship between conscientiousness information security awareness does not exist.

H_{A3}: A statistically significant relationship between extraversion and information security awareness does exist.

H_{03}: A statistically significant relationship between extraversion and information security awareness does not exist.

H_{A4}: A statistically significant relationship between agreeableness and information security awareness does exist.

H_{04}: A statistically significant relationship between agreeableness and information security awareness does not exist.

H_{A5}: A statistically significant relationship between neuroticism and information security awareness does exist.

H_{05}: A statistically significant relationship between neuroticism and information security awareness does not exist.

Research Question 2: What is the relationship between generational cohort, measured as a categorical variable, and information security awareness?

H_A: Generational cohort, measured as a categorical variable, is statistically related to information security awareness.

H_0: Generational cohort, measured as a categorical variable, is not statistically related to information security awareness.

Research Question 3: Does generational cohort, measured as a categorical variable, moderate the relationship between personality and security awareness?

H_{A1}: Generational cohort does moderate the relationship between openness and information security awareness.

H_{01}: Generational cohort does not moderate the relationship between openness and information security awareness.

H_{A2}: Generational cohort does moderate the relationship between conscientiousness and information security awareness.

H_{02}: Generational cohort does not moderate the relationship between conscientiousness and information security awareness.

H_{A3}: Generational cohort does moderate the relationship between extraversion and information security awareness.

H_{03}: Generational cohort does not moderate the relationship between extraversion and information security awareness.

H_{A4}: Generational cohort does moderate the relationship between agreeableness and information security awareness.

H_{04}: Generational cohort does not moderate the relationship between agreeableness and information security awareness.

H_{A5}: Generational cohort does moderate the relationship between neuroticism and information security awareness.

H_{05}: Generational cohort does not moderate the relationship between neuroticism and information security awareness.

Once the survey was deployed and the number of survey participants was reached, the results were compiled for review. Using the data collected, the analysis and examination of the data and removed any identified incomplete data. One method of analysis used correlation analyses to examine the strength of the relationship between the variables. Another technique was using linear regression to examine the criterion and predictor variables to see a significant association. Linear regression also examined the variance found in perceived barriers in the self-reported behaviors of information security awareness and personality traits.

Assumptions were made concerning the linear regression model for the relationship between the criterion and predictor variables. Regression analysis helps test the hypotheses. Multiple linear regression analysis is often used to analyze experimental and nonexperimental designs (Green & Salkind, 2010). The evaluation of the data examined the assumptions of multiple regression and moderated multiple regression using the Hayes Process macro.

There were two assumptions for multiple regression normality and homogeneity of variances. Normality is data that has a normal distribution or is symmetric. Homogeneity of variances is data from various groups that have the same variance. An evaluation of the data, and a descriptive summary was be used for statistical analysis.

Violation of assumptions impacts the data validity and results. There are recommendations for those cases concerning the assumption of normality to transform data busing natural log or square root transformations (Rummel, 1988). If necessary, the Bonferroni Correction can be used to correct or control for Type I errors. Warner (2013)

discusses the need to utilize a correction method for analyzing variance in multiple comparison schemes, particularly univariate methods, where Type I errors occur.

Creating confounders to control was critical for reliable causal inference (VanderWeele, 2016). Confounder variables affect the variables in the study, so the results do not reflect a relationship. The research may rely on statistical methods to adjust the confounding effects in premature or impossible experimental designs.

Ethical Procedures

The concern regarding ethics arise due to factors found during the research process. Approval obtained from Walden University IRB (Approval no. 03-08-22-0752485) before the start of this study was the beginning of the process. Ethical issues arise when conducting online research and are unique in areas of conformity of adult participants. Online research presents difficulties in confirming if the participants are within the age groups specified. To ensure the participants were protected, documentation relating to their privacy, informed consent, and full disclosure will allow participants to understand their rights. No incentives were provided for any participation in the study. Participants could withdraw from the study at any point during the process. In addition, participants received contact information for Walden University if they wanted additional information regarding the survey.

The survey tool SurveyMonkey utilizes Secure Socket Layers encryption that allows participants' responses to be encrypted to ensure their privacy (SurveyMonkey, 2019). The survey tool, Facebook, also offers privacy to the online partners by preventing personal information between Facebook and its advertisers (Facebook, 2013). The

advertisements can be hidden from the participants or blocked to allow control of data displayed to users. The participants' privacy was essential, and confidential information was protected using secure password protection and that the electronic data was stored on a password-protected external hard drive. The participant's information requires destruction after five years.

Summary

While personality and prior generational cohorts have studied, there needs to be more research on Generation Z. Moreover, there is very little research on how generations and personalities interact to impact information security. The research study utilized a quantitative design and examined the factors determining personality traits associated with generations and information security awareness. The research explored the relationship between personality traits and generational cohorts in the workplace regarding how these may impact information security awareness. The relationship between personality and information awareness was explored in research presented by Parsons et al. (2017), knowledge of information security policy influenced attitudes. While the impact of personality on information security awareness was explored in research, consideration of which generational cohorts contribute is not a typical research area.

The research questions assessed the personality trait and information security awareness of multiple generations using the generational cohort theory and Five Factor Model. The survey was distributed to social media and online groups using the SurveyMonkey online survey site. SPSS was used to analyze the data from the

participants after IRB approval was obtained. And the determination of ethical guidelines was followed pertaining to participants. In Chapter 4, the three research questions and hypotheses and discuss the results from the survey. Chapter 4 also contains an analysis of the data and the tests of the three hypotheses. The chapter concludes with a summary of the analysis.

Chapter 4: Results

This chapter discusses the outcome that will assist in better understanding the relationship between personality traits and information security awareness for multiple generations. The research used a quantitative method approach using Parsons et al. (2017), the HAIS-Q, and five-factor model from Costa and McCrae (2008). The HAIS-Q was used to capture the knowledge, attitude, and behaviors related to information security awareness, whereas the FFM was used to measure the personality traits: openness, contentiousness, extroversion, agreeableness, neuroticism.

Chapter 4 includes a summary of the data collection, which discusses the recruitment process, the demographic profile of the sample, and descriptive statistics for the measures. The sample was largely Generation Y at 40%, followed by Generation X at 30%. The chapter will also cover the descriptive results and results from the multiple regression analysis used to test the hypotheses.

Data Collection

The collection involved contacting multiple online groups using social media and posting the invitation to solicit participation in the study. The Walden IRB approved the approach of asking group administrators for permission to post the survey in their groups. The request asked for participants to be over the age of 18, and that they are working with computers/technology or information security.

The SurveyMonkey survey platform hosted the survey. A link was provided to the survey included in the invitation. Data collection began on March 8, 2022, and was completed on June 18, 2022. Of the 137 individuals that began the survey, 20 did not

complete it, resulting in 117 participants who completed the survey for a completion rate of 85.4%. A few demographic questions were asked but no personally identifying data were collected.

The survey started with the informed consent form that the participants had to acknowledge to begin the survey. The participants then proceeded to the demographic questions such as age, work experience, current employment, household income, and gender. The following section included questions from Parsons et al.'s (2017) HAIS-Q survey tool that looked at information security awareness statements where they were ranked on a Likert scale. The categories contained in the Information Security Awareness (ISA) tool looked at email security, computer use, internet use, social media, mobile devices, information handling, and incident reporting. The section focuses on security as contained in a group of questions that indicated the perception level of the respondent. Finally, the last section included personality questions from John and Srivastava's (1999) BFI, where participants were again able to use a Likert scale to rate their personality based on five personality traits: openness, conscientiousness, extraversion, agreeableness, and neuroticism. Each participant had the option of leaving the survey at any time.

Demographics

The first section of the survey provided six demographic questions for each participant to answer. The questions established background information and age that was asymulated into generational cohorts. The participants' responses are identified and presented in Tables 1–6.

- Generational cohorts: 22.6% of the participants were in Generation Z, 29.9% were millennials and Generation X, and baby boomers made up 17.5% of the cohorts.
- Gender: 73.7% of the respondents were female.
- Employment status: 70.1% of the participants were employed full-time.
- Education level: 40.1% of the participants held a master's degree.
- Income range: The highest household income was between $100,000 and 150,000.

The first demographic question identified the age of the participants. There were 54 possible answers derived for the age groups ranging from 18 to over 70. The individual ages were grouped into generational cohorts as shown in Table 1.

Table 1

Generational Cohort Distribution of the Sample

Generation name	Frequency	%	Valid %
Generation Z	31	22.6	22.6
Millennials	41	29.9	29.9
Generation X	41	29.9	29.9
Baby boomers	24	17.5	17.5

The second question asked the gender of the participant (see Table 2). The results were that participants were predominantly female with 73.7%, whereas 23.4% were male. There were an additional 3% who were self-described or preferred not to answer. There was no specific focus for gender in the survey, the results were not expected for the female to male ratio.

Table 2

Gender Distribution of the Sample

Gender	Frequency	%	Valid %
Female	101	73.7	73.7
Male	32	23.4	23.4
Self-described	2	1.5	1.5
Prefer not to answer	2	1.5	1.5
Total	137	100.0	100.0

The third demographic question requested highest level of educational (see Table 3). There were six answers available for responses. All participants responded, and the largest percentage (40.1%) indicated having obtained their master's degree, followed by 38% with a bachelor's degree.

Table 3

Education Status of the Sample

Educational status	Frequency	%	Valid %
High school	12	8.8	8.8
Associate degree	14	10.2	10.2
Bachelor degree	52	38.0	38.0
Master degree or higher	55	40.1	40.1
Other	2	1.5	1.5
Prefer not to answer	2	1.5	1.5
Total	137	100.0	100.0

The fourth demographic question was about the employment status (see Table 4). One participant did not answer the question. The majority of participants (70.1%) were employed full time.

Table 4

Employment Status Distribution of the Sample

Employment status	Frequency	%	Valid %
Full-time	96	70.1	70.6
Part-time	13	9.5	9.6
Not employed	21	15.3	15.4
Other	5	3.6	3.7
Prefer not to answer	1	0.7	0.7
Valid response total	136	99.3	100.0
No response	1	0.7	
Total sample	137	100.0	

The fifth question focused on the number of years of employment in the information security or working with security measures (see Table 5). This question was broken down into the number of years ranging from 1 to over 31 years. The highest results show that 48.2% have only been in the field for 1–10 years.

Table 5

Years of Employment of the Sample

Work experience	Frequency	%
1–10 years	66	48.2
11–20 years	36	26.2
31+ years	11	7.9
Total	126	91.7
Missing system	11	8.3
Total	137	100

The final question addressed household income (see Table 6). The income ranges were broken down into multiple income ranges. The highest percentage of participants (21.2%) were in the income range of $100,000 to $150,000.

Table 6

Household Income of the Sample

Household income	Frequency	%
Under $15,000	18	13.1
Between $15,000 and $29,999	7	5.1
Between $30,000 and $49,999	23	16.8
Between $50,000 and $74,999	17	12.4
Between $75,000 and $99,999	17	12.4
Between $100,000 and $150,000	29	21.2
Over $150,000	24	17.5
Total	135	98.5
No response	2	1.5
Total sample	137	100

Main Study

The mean and standard deviation for generational cohort was found using SPSS software. The mean of the cohorts is found in Table 7 along with other descriptive information. The calculated mean and standard deviation score for millennials and ISA were $M = 12.23$ and $SD = 2.28$. The values for Generation X and ISA were $M = 13.02$ and $SD = .83$. Baby boomer values were $M = 12.89$ and $SD = .83$.

Table 7

Descriptive Statistics for Generational Cohort

	Millennials		Generation X		Baby boomers		Combined
Variable	*M*	*SD*	*M*	*SD*	*M*	*SD*	alpha
Information security awareness	12.23	2.28	13.02	.83	12.89	.83	.08
Extraversion	2.77	.82	3.05	.88	3.30	.78	.03
Agreeableness	3.85	.43	3.96	.55	4.12	.57	.04
Openness	3.56	.42	3.68	.48	3.62	.43	.05
Neuroticism	3.10	.82	2.63	.83	2.56	.81	.109
Conscientiousness	3.83	.66	4.09	.56	4.27	.54	.03

The correlation portion of the sample was determined using SPSS software. Table 8 provides the Pearson correlation between ISA, BFI, and generational cohort. The correlation for cohort and ISA ($r = .18$, $p < .05$), which provided support to reject the null hypothesis. In addition, the Pearson correlation for BFI and ISA variables (agreeableness, extraversion, conscientiousness, neuroticism, and openness) are included in Table 8. Of the subsequent five variables, two were statistically significant.

Table 8

Pearson's Correlation of Sample

Variable	Cohort	ISA	Agreeableness	Extraversion	Conscientiousness	Neuroticism	Openness
Cohort	1	.18*	.23*	.22*	.32**	-.26**	.16
ISA	.18*	1	.23*	.18	.11	-.13	.19
Agreeableness	.23*	.23*	1	.29**	.51**	-.36**	.13
Extraversion	.22*	.18	.29**	1	.26**	-.50**	.33**
Conscientiousness	.32**	.11	.26**	.26**	1	-.40**	.19*
Neuroticism	-.26**	-.13	-.36	-.50**	-.40**	1	-.19*
Openness	.16	.19*	-33**	.33**	.19*	-.19	1

Note. $N = 117$; ISA = information security awareness.
* $p < .05$, ** $p < .001$

The reliability was determined using SPSS software. Part 1 of the survey, Parsons et al.'s (2017) HAIS questionnaire, had 28 questions that participants responded using a 7-point Likert scale. A Cronbach's measured the internal consistency for internal security awareness was measured resulting in .79 for the 28 items on Part 1 of the survey. Part 2 of the survey addressed the BFI personality traits. Cronbach's alpha reliability coefficient of .69 was the output for the 44 items in Part 2 of the survey. Table 9 shows the Cronbach's α values and alpha for standardized items in the reliability output.

Table 9

Cronbach's Alpha for Survey

	N of participants	%	Cronbach's α	α standardized items	*N* of items
Part 1:ISA	118	86	.79	.83	28
Part 2: BFI	107	78	.69	.74	44

Information Security Awareness

The second measure of the survey used Parsons et al. (2017) HAIS questionnaire to look at how the independent variable in the study, internal and external inherent factors affected the participants level of security awareness. The survey used descriptives to measure the knowledge, attitude, or behavior of each participants level of security awareness.

Personality Traits

The third section of the survey looked at personality traits using John and Srivastava's (1999) five personality constructs: openness, conscientiousness, extraversion, agreeableness, and neuroticism. The responses in each section used a Likert scale from 1 to 5, with 1 being the strongest disagreement and 5 being the strongest agreement. Each of the responses in the personality section was assessed from the lowest possible score of 5 and the maximum score of 25.

Discrepancies in Data

The data collection process followed the plan presented in Chapter 3, with one exception. It was planned to have approximately equal numbers of people in all four generations: baby boomers, Generation X, millennials, and silent. However, only two

people in the silent generation responded to the survey. And 31 participants responded from Generation Z. This resulted in only three generation groups for analysis. Also, the for the original proposal, I assumed that the rate of Generation X and millennials participants in the survey would be similar to that of other generations. However, Generation X and millennials presented a 29.9% participation rate for the survey. In addition, the silent and baby boomer representation was not separated into the upper age divisions. Not representing the appropriate age groups and not accounting for Generation Z, presented 22.6% of the participants not accounted in this study and two not properly categorized and accounted in the survey.

Testing Assumptions for Regression

This study had two scores for the independent variable (personality and generational cohort). There was one dependent variable (information security awareness). First, the analysis was used as an assessment of the suitability of the data for regression. The generated results from the regression procedure indicated there was no significant differences, $F(1, 120) = 3.94$, $p \leq .05$, in the information security awareness due to generational cohort status. A summary of the results is depicted in Table 10.

Table 10

Predicting Information Security Awareness from Generational Cohort

Dependent variable	*SS*	*df*	*MS*	*F*	Sig
Regression	684.03	1	684.03	3.94	.049
Residual	20825.85	120	173.55		
Total	21509.88	121			

The generated results from the linear regression procedure indicated there were no significant differences, $F(1, 115) = 3.84$, $p \geq .05$, in the information security awareness due to personality trait extraversion (see Table 11).

Table 11

Regression Between Information Security Awareness for Extraversion

	SS	*df*	*MS*	*F*	Sig
Regression	2.71	1	2.709	3.841	.052
Residual	81.09	115	.71		
Total	83.78	116			

The generated results from the regression procedure indicated there were no significant differences, $F(1, 115) = 6.39$, $p \leq .05$, in the information security awareness due to personality trait agreeableness (see Table 12).

Table 12

Regression Between Information Security Awareness for Agreeableness

Dependent variable	*SS*	*df*	*MS*	*F*	Sig
Between groups	1.67	1	1.67	6.387	.013
Within groups	30.13	115	.262		
Total	31.81	116			

The generated results from the procedure indicated there were no significant differences, $F(1, 115) = 1.41$, $p \geq .05$, in the information security awareness due to personality trait conscientiousness (see Table 13).

Table 13

Regression Between Information Security Awareness for Conscientiousness

Dependent variable	*SS*	*df*	*MS*	*F*	Sig
Regression	.57	1	.57	1.41	.24
Residual	46.56	115	.41		
Total	47.13	116			

The generated results from the procedure indicated there were no significant differences, $F(1, 115) = 1.96$, $p \geq .05$, in the information security awareness due to personality trait neuroticism (see Table 14).

Table 14

Regression Between Information Security Awareness for Neuroticism

Dependent variable	*SS*	*df*	*MS*	*F*	Sig
Regression	1.38	1	1.38	1.95	.17
Residual	81.5	115	.71		
Total	82.881	116			

The generated results from the procedure indicated there were no significant differences, $F(21, 95) = 1.26$, $p \geq .05$, in the information security awareness due to personality trait openness (see Table 15).

Table 15

Regression Between Information Security Awareness for Openness

Dependent variable	*SS*	*df*	*MS*	*F*	Sig
Between groups	36.78	21	1.75	1.26	.22
Within groups	131.75	95	1.39		
Total	168.53	116			

Results

This section reports the results of the sample description from the survey. The discussion of the prescreening of respondents and a summary of demographic data captured. The evaluation of research questions shows the finding concerning the research questions. The research questions address each generational cohort, personality trait, and information security awareness.

Sample Description

The survey captured basic demographic information from the respondents. The participants were required to be 18 years old and working with computers/technology or information security. The first demographic question identified the age of the participants by asking them to provide their age as an integer. There were fifty-four possible answers derived for the age groups ranging from 18 to over 70. The individual ages were grouped into generational groups to correspond to the appropriate cohort. The second question asked about the gender of the participant. The results were predominantly female with 73.7% and male with 23.4%. There was an additional 3% that were self-described or preferred not to answer. There was no specific focus on gender in the survey, and the results were not expected for the female-to-male ratio. The third demographic question requested the highest level of education. There were six answers available for responses. All participants responded, and the majority indicated that 40.1% obtained their master's degree, followed by 38% obtaining their bachelor's degree. The fourth demographic question examined employment status. One participant did not answer the question. Most participants were employed showed, 70.1%. And the fifth question focused on the

number of years of employment in information security or working with security measures. This question was broken down into years ranging from one year to over 40 years. The results show that 13.9% have only been in the field for one year. The final question asked respondents to indicate their household income. Two respondents did not respond to the question. The highest household income bracket shows 21.2% between $100,000 and 150,000. The lowest income bracket shows under $15,000 at 13.1%.

Evaluating Research Questions

This section analyzes the research questions for this study focused on the two independent variables, generational cohort and personality traits, and their relationship with the dependent variable, information security awareness level. This was reported on each generational cohort. The research questions were used to understand the relationship between generational cohorts, personality traits, and information security awareness in the following questions and hypotheses:

Research Question 1:

What is the relationship between personality and information security awareness?

Hypotheses:

H_{A1}: A statistically significant relationship between openness and information security awareness does exist.

H_{01}: A statistically significant relationship between openness and information security awareness does not exist.

H_{A2}: A statistically significant relationship between conscientiousness and information security awareness does exist.

H_{02}: A statistically significant relationship between conscientiousness information security awareness does not exist.

H_{A3}: A statistically significant relationship between extraversion and information security awareness does exist.

H_{03}: A statistically significant relationship between extraversion and information security awareness does not exist.

H_{A4}: A statistically significant relationship between agreeableness and information security awareness does exist.

H_{04}: A statistically significant relationship between agreeableness and information security awareness does not exist.

H_{A5}: A statistically significant relationship between neuroticism and information security awareness does exist.

H_{05}: A statistically significant relationship between neuroticism and information security awareness does not exist.

The first research question inquired about the extent if at all, there was a relationship between personality and information security awareness. Linear regression was conducted with the result for openness, $F(1,115) = 4.11$; $p \geq .05$). The result for agreeableness, $F(1,115) = 6.39$, $p < .05$, and for extraversion, $F(1,115) = 1.96$, $p \leq .05$, indicated there is a significant difference between the groups and the null hypothesis is rejected. The null hypothesis for conscientiousness and neuroticism shows no statistical difference from zero. Table 16 includes the results of each personality trait with information security awareness.

Table 16

Predicting Information Security Awareness from Personality

Predictor	*B*	*df*	*MS*	*F*	*p*	Adj. R^2	*T*	*p*
Openness	10.87	1	5.81	4.11	.05	.03	2.03	.05
Conscientiousness	11.93	1	2.04	1.41	.24	.00	1.19	.24
Extraversion	11.99	1	5.48	3.8	.05	.02	1.96	.05
Agreeableness	10.68	1	8.87	6.39	.01	.04	2.53	.01
Neuroticism	13.28	1	2.80	1.95	.17	.01	-1.40	.17

Information security awareness had seven categories with three sub-categories. A dummy variable was created for each category to better quantify the relationship between the variables.

Research Question 2:

What is the relationship between generational cohort, measured as a categorical variable, and information security awareness?

Hypotheses:

H_A: Generational cohort, measured as a categorical variable, is statistically related to information security awareness.

H_0: Generational cohort, measured as a categorical variable, is not statistically related to information security awareness.

The second research question inquired the extent if at all, there was a relationship between generational cohort and information security awareness. There is no statistical difference from zero. Table 17 shows the results of generational cohort and information security awareness.

Table 17

Cohort and Information Security Awareness

Predictor	*B*	*df*	*MS*	*F*	*p*	Adj. R^2	*T* value	*p*
Generation cohort	12.12	1	6.38	2.49	.12	.01	1.58	.12

Research Question 3:

Does generational cohort, measured as a categorical variable, moderate the relationship between personality and security awareness?

Hypotheses:

H_{A1}: Generational cohort does moderate the relationship between openness and information security awareness.

H_{01}: Generational cohort does not moderate the relationship between openness and information security awareness.

H_{A2}: Generational cohort does moderate the relationship between conscientiousness and information security awareness.

H_{02}: Generational cohort does not moderate the relationship between conscientiousness information security awareness.

H_{A3}: Generational cohort does moderate the relationship between extraversion and information security awareness.

H_{03}: Generational cohort does not moderate the relationship between extraversion and information security awareness.

H_{A4}: Generational cohort does moderate the relationship between agreeableness and information security awareness.

H_{04}: Generational cohort does not moderate the relationship between agreeableness and information security awareness.

H_{A5}: Generational cohort does moderate the relationship between neuroticism and information security awareness.

H_{05}: Generational cohort does not moderate the relationship between neuroticism and information security awareness.

The third research question inquired if generational cohort moderates, if at all, the relationship between personality and information security awareness. The conclusion is that openness does moderate the relationship between personality and information security awareness. Based on the statistical significance value of $p < .05$, there is no statistical difference from zero. Table 18 shows the results of moderation by generational cohort on personality and information security awareness.

Table 18

Moderation Analysis Summary

Predictor	*B*	*df*	*MS*	*F*	*p*	Adj. R^2	*T* value	*p*
Generation Cohort	1.74	3	4.14	3.0	.03	.05	2.04	.04
Openness	1.76						2.50	.01
Generation Cohort X Openness	-.44						-1.95	.05
Generation Cohort	.57	3	1.6	1.13	.34	.00	1.19	.23
Conscientiousness	.73						1.31	.19
Generation Cohort X Conscientiousness	.16						-1.07	.29
Generation Cohort	.11	3	2.20	1.54	.21	.01	.29	.77
Extraversion	.25						.73	.47
Generation Cohort X Extraversion	-.01						-.07	.94
Generation Cohort	1.07	3	4.34	3.15	.03	.05	1.6	.10
Agreeableness	1.28						2.37	.02
Generation Cohort X Agreeableness	-.26						-1.59	.11
Generation Cohort	-.1	3	1.57	1.08	.36	.00	-.30	.77
Neuroticism	-.35						-1.00	.32
Generation Cohort X Neuroticism	.07						.61	.55

Summary

Chapter 4 provided a compilation and presentation of the data collected using statistical analyses. The study included a collection of demographic data from three generational cohorts. A total of 117 individuals who completed surveys to determine the relationship between the predictor variables, generational cohort, and personality traits were measured and computed. The criterion variable information security awareness used to measure relationships between the predictor variable generational cohort and personality trait. Descriptive data were utilized to portray the data concisely.

Research Question 1 showed a statistical relationship between openness and agreeableness. Research Question 2 addressed the relationship between generational cohort and information security awareness. There was no statistical difference shown for Question 2. Chapter 5 summarizes the study, provides suggestions, and offers conclusions. Chapter 5 also identifies the social change implications of this study.

Chapter 5: Discussion, Conclusions, and Recommendations

In past studies, researchers have investigated the personality traits and generational differences in information security awareness (Cekada, 2012; Cogin, 2012; Costa & McCrae, 2008; Jiang et al., 2016). Individual personality traits were found to impact information security awareness within organizations using the HAIS-Q (Parsons et al., 2014). Therefore, as a new generation joins the workforce, further research must be done to investigate the level to which employees in new and existing generational cohorts differ in an organization's commitment and the impact they can have on an organization's information security awareness.

This quantitative study aimed to determine if there was a significant difference in information security awareness for four generational cohorts (millennials, Generation X, baby boomer, and silent generations), along with the impact of personality traits on information security awareness. Results from the demographic data revealed that most participants were female full-time employees with master's degrees and working in technology for up to 10 years. The data also showed that millennials and Generation X composed the largest generational cohort. From the data analysis, the silent generation comprised the smallest group and was excluded from the data analysis. This chapter presents the limitations of the study, implications for social change, and suggestions for future research.

Interpretation of the Findings

The central premise of the study was that personality traits and generational cohorts impact information security awareness. Results from past studies show that

generational cohorts have experienced shared life events, and these experiences have had an effect on shaping their belief systems and values (Jiang et al., 2016; McCrae, 2018; Wiley, McCormac, & Calic, 2020; Wiley, McCormac, & Calic, 2020). The differences found in generational cohorts are based on life events. Life events such as social, economic, political, and economic standing during their early development impact their perspectives. The impact of those events affects both how people live and how people respond in work environments.

Each generation had events that impacted their personality, such as past experiences, historical events, and beliefs (Clark, 2017). Personality traits have been found to predict cybersecurity behavior. Shappie et al. (2019) utilized BFI to measure self-reported cybersecurity behaviors and found that most factors associated with those behaviors were conscientiousness, agreeableness, and openness. Therefore, it is crucial to understand each generational cohort and personality trait to shape the uniqueness found in each.

The first research question addressed the relationship between personality measured by the five-factor model used by McCrae and John (1992) and information security awareness (Parsons et al., 2014). Shappie et al. (2019) found conscientiousness and openness to be the common personality traits in measuring the relationship between personality traits and cybersecurity behaviors. In another study, Shropshire et al. (2015) found that conscientiousness and agreeableness influenced security attitudes, intentions, and behavior in security attitudes. The study also showed that those traits increased

intention and initial adherence to security practices (Shappie et al., 2019; Shropshire et al., 2015).

The first research question result from this study showed that agreeableness was the only personality trait where the null hypothesis was not accepted. As a result, openness, agreeableness, and extraversion were found to have no statistically significant differences in information security awareness. These results are different in that conscientiousness and neuroticism was not statistically significant.

The second research question addressed to what extent, if at all, there was a relationship between generational cohort and information security awareness. Regression was utilized to test the three variables (information security awareness, generational cohort, personality trait) was significantly different. The results revealed no statistical difference from zero found with the variables.

The third research question inquired if generational cohort moderates, if at all, the relationship between personality and information security awareness. Research findings by Cunningham et al. (2018) and Thompson et al. (2017) found that personality may predict cybersecurity behavior. Shappie et al. (2019) also found that personality predicts behavior and also compliance with risk to data and safety measures. Organizations with cyber threats had a 95% result with users and poor cybersecurity skills, according to Carlton et al. (2019). The analysis showed no significant moderating effect of openness on the relationship between generational cohort and information security awareness.

Limitations of the Study

The study had limitations on the number the participants, and some did not complete the survey. Furthermore, the participants may not have answered the questions honestly. The limitations could be due to several possibilities ranging from the desire not to reveal personal information, weaknesses, or incompetency. Other limitations may affect the findings of this study. The first limitation pertained to the age of participants. Chapter 2 details how the silent generation could impact the study's findings. From observation, gender also played a role in the study, with the majority being female.

The study explored the impact age had on information security awareness. The second limitation pertains to limiting the age for participants under age 22. Consequently, a study's result may not compare to other samples. The study indicated that millennials had more information security awareness. Previous studies presented by Cogin (2022) showed a decline in work ethics by millennials.

A third limitation of the study was the sample size. The G-Power tool was utilized to find the study's sample and effect size. The G*Power tool is a software or calculator based on the input to support the probability distributions (Erdfelder et al., 1996). The overarching sample size met the minimum criteria established in the G-Power analysis and presented a 95% possibility. The small sample could impact the findings found in this study if taken from a different sample. The program can also display relations in variables graphically (Erdfelder et al., 1996).

The study contained demographic questions that asked about the gender of the participants. The demographic questions posed a limitation that pertains to gender ratios.

The male-to-female ratio was unexpected and not the focus of the study. This research survey contained predominantly females, with 73.7% of the participants. Male participants resulted in 23.4%. Future examination of gender differences in information security awareness poses a topic for investigation. According to Anwar et al. (2017), women comprise 47% of the workforce, and gender is statistically significant.

Recommendations

The following recommendations are offered to address the abovementioned limitations and future study considerations. There should be no limitation on the age of participants, and include all likely ages in future research. For example, the silent generation is a small sample size, and baby boomers will be exiting the workforce soon. The silent generation age group ranges from 78 to 95, and they have predominately left the workforce. Baby boomers, ages ranging from 59 to 77, have begun to leave the workforce and will continue over the next 10 or more years. For future workforce, the focus should be on Generation X, Y, and Z and those coming behind those generations. Finally, further research would benefit from a larger sample of each generation to assess whether there is replication in the study.

Implications

The study contributes to understanding how, if at all, generational cohorts impact information security awareness. Prior research has shown concern that cohorts are the link that could change the security posture of systems (Shappie et al., 2019). Another study found that online safety and training were a factor in lacking to change in the online security culture (Jiang et al., 2016; Marangione, 2019; Viega, 2018). The prior studies

contained different outcomes. This study's results suggest that generations have no bearing on information security awareness. The results might infer that generations do not impact information security awareness or other organizational security outcomes.

The results from the study promote social change and may find this study helpful by providing insight concerning how generational cohorts have no bearing on information security awareness. Furthermore, organizations should be confident when hiring cohorts to exist among organizations. Individuals in the field of information security awareness should continue introducing new ways of social change.

Organizations foster positive social change by engaging employees in finding solutions to security breaches for the foreseeable future as technology continues to become prominent in society and organizations. Finally, organizations can promote positive social change among up to three generations that coexist in the workforce through adaptation and technology changes through training.

Conclusion

In organizations today, people work with multiple generations and in information-rich areas. Technology will continue to be complex for people and systems within those organizations and collaboration among cohorts. This quantitative study aimed to determine whether there were significant differences in personality traits found in four generational cohorts (Generation X, millennials, baby boomers, and silent). This study also investigated whether generational cohorts impacted information security awareness. The data showed that awareness moderates the relationship between personality and

information security awareness. The results showed that Generation X and millennials had the highest levels of information security awareness.

References

Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020). Internet of things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*, *54*, Article 101728. https://doi.org/10.1016/j.scs.2019.101728

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Bakker, A. B., Van Der Zee, K. I., Lewig, K. A., & Dollard, M. F. (2006). The relationship between the big five personality factors and burnout: A study among volunteer counselors. *The Journal of social psychology, 146*(1), 31-50.

Banomyong, R., Varadejsatitwong, P., & Oloruntoba, R. (2019). A systematic review of humanitarian operations, humanitarian logistics and humanitarian supply chain performance literature 2005 to 2016. *Annals of Operations Research*, *283*(1/2), 71–86. https://doi.org/10.1007/s10479-017-2549-5

Beuran, R., Pham, C., Tang, D., Chinen, K.-i., Tan, Y., & Shinoda, Y. (2018). Cybersecurity education and training support system: CyRIS. *IEICE TRANSACTIONS on Information and Systems*, *E101D*(3), 740-749. https://doi.org/10.1587/transinf.2017edp7207

Becerra-García, J. A., García-León, A., Muela-Martínez, J. A., & Egan, V. (2013). A controlled study of the Big Five personality dimensions in sex offenders, non-sex offenders and non-offenders: relationship with offending behaviour and childhood

abuse. *The Journal of Forensic Psychiatry & Psychology, 24*(2), 233–246. https://doi.org/10.1080/14789949.2013.764463

Bernard, H. R. (2013). *Social research methods: Qualitative and quantitative approaches.* Sage.

Boyle, T., Grieshaber, S., & Petriwskyj, A. (2018). An integrative review of transitions to school literature. *Educational Research Review*, *24*, 170–180. https://doi.org/10.1016/j.edurev.2018.05.001

Burkholder, G., Cox, K., & Crawford, L. (2016). The scholar-practitioner's guide to research design (1st ed). Laureate Publishing.

Brutus, S., Aguinis, H., & Wassmer, U. (2013). Self-reported limitations and future directions in scholarly reports analysis and recommendations. *Journal of Management, 39*, 48-75. https://doi-org.ezp.waldenulibrary.org/10.1177/0149206312455245

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyberattacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*, *27*(1), 101-121. https://doi.org/10.1108/ICS-11-2016-0088

Cekada, T. L. (2012). Training a multigenerational workforce. *Professional Safety, 57*(3), 40-44.

Clark, K. (2017). Managing multiple generations in the workplace. *Radiologic Technology, 88(4),* 379-398.

Cogin, J. (2012). Are generational differences in work values fact or fiction? Multi-country evidence and implications. *The International Journal of Human Resource Management, 23*(11), 2268-2294. https://doi.org/10.1080/09585192.2011.610967

Connolly, J. (2019). Generational conflict and the sociology of generations: Mannheim and Elias reconsidered. *Theory, Culture & Society, 36*(7/8), 153–172. https://doi.org/10.1177/0263276419827085

Costa, P. T., & McCrae, R. R. (2008). The revised NEO personality inventory (NEO-PI-R). In G. J. Boyle, G. Matthews, & D. H. Saklofske (Eds.), *The SAGE handbook of personality theory and assessment. Vol. 2, Personality measurement and testing* (pp. 179–198). SAGE Publications.

Cram, W. D. A. J., & Proudfoot, J. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly, 43*(2), 525–554. https://doi.org/10.25300/MISQ/2019/15117

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297-334.

Cunningham, M. R., Jones, J. W., & Dreschler, B. W. (2018). Personnel risk management assessment for newly emerging forms of employee crimes. *International Journal of Selection & Assessment, 26*(1), 5-16. https://doi.org/10.1111/ijsa.12202

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7.

Dimock, M. (2018). Defining generations: Where millennials end and post-millennials begin. Fact Tank: News in the Numbers. *Pew Research.* http://www.pewresearch.org/facttank/2018/03/01/defining-generations-where-millennials-end-and-post-millennials-begin/

Edmunds, J., & Turner, B. S. (2005). Global generations: social change in the twentieth century. *The British journal of sociology, 56*(4), 559-577.

Erdfelder, E., Faul, F., & Buchner, A. (1996). Gpower: A general power analysis program. *Behavior Research Methods, Instruments, & Computer, 28*, 1-11. https://doi.org/10.3758/BF03203630

Facebook. (2019). *Facebook Ads: Reach out to future customers and fans*. Retrieved January 2021, from https://www.facebook.com/business/ads

Fleeson, W., & Jayawickreme, E. (2015). Whole trait theory. *Journal of Research in Personality*, *56*, 82–92. https://doi.org/10.1016/j.jrp.2014.10.009

Goldberg, L. R. (1993). The structure of phenotypic personality traits. *American psychologist, 48*(1), 26.

Göncz, L. (2017). Teacher personality: a review of psychological research and guidelines for a more comprehensive theory in educational psychology. *Open Review of Educational Research, 4*(1), 75–95. https://doi.org/10.1080/23265507.2017.1339572

Gosling, S. D., Rentfrow, P. J., & Swann, W. B. Jr. (2003). A very brief measure of the Big-Five personality domains. *Journal of Research in personality, 37*(6), 504-528.

Green, S. B., & Salkind, N. J. (2010). *Using SPSS for Windows and Macintosh: Analyzing and understanding data*. Prentice Hall Press.

Houck, C. (2011). Multigenerational and virtual: How do we build a mentoring program for today's workforce? *Performance Improvement, 50*(2), 25-30. https://doi.org/10.1002/pfi.20197

Howe, N., & Strauss, W. (2007). THE BIG PICTURE. *The next, 20*, 8-7.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security,* 31(1), 83-95. http://dx.doi.org/10.10106/j.cose.2011.10.007

Jenab, K., & Moslehpour, S. (2016). Cyber security Management: A review. *Business Management Dynamics, 5*(11), 16-39.

Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. Information & Management, 56(5), 681-695. https://10.1016/j.im.2018.11.003

Jiang, M., Tsai, H. S., Cotten, S. R., Rifon, N. J., LaRose, R., & Alhabash, S. (2016). Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology, 42*(9), 621–634. https://doi.org/10.1080/03601277.2016.1205408

John, O. P., & Srivastava, S. (1999). The big five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin and O. P. John (Eds.), *Handbook of personality theory and research.* The Guilford Press.

Kersting, L. M. (2003). *Adult children of late parental divorce: A comparison of younger and older adults.* Massachusetts School of Professional Psychology.

Kim, H. E., Son, H. S., Kim, J., & Kang, H. G. (2017). Systematic development of scenarios caused by cyberattack-induced human errors in nuclear power plants. *Reliability Engineering and System Safety*, *167*, 290–301. https://doi.org/10.1016/j.ress.2017.05.046

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security, 59*(3), 60-70. https://doi.org/10.1016/j.cose.2016.02.004

Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the castle model of cyber-risk and cybersecurity. *Government Information Quarterly, 33*(2), 250-257. https://doi.org/10.1016/j.giq.2016.01.012

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

LinkedIn. (2019). *How LinkedIn can help you*. https://linkedincom/help/linkedin/answer/45/how-linkedin-can-help-you?lang=en

Liu, L., Li, Y., Li, S., Hu, N., He, Y., Pong, R., … & Law, M. (2012). Comparison of next-generation sequencing systems. *Journal of Biomedicine and Biotechnology, 2012.*

Maddison, J. (2018). Evolving security for digital transformation. *ISSA Journal, 16*(4), 29.

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for 85optimizing cybersecurity practices. *Computers & Security*, *95,* 1-17. https://doi.org/10.1016/j.cose.2020.101846

Mannheim, K. (1952). The problem of generations. In *Essays on the Sociology of Knowledge,* 276-320.

Marangione, M. (2019). Millennials: Truthtellers or threats? *International Journal of Intelligence and CounterIntelligence, 32*(2), 354-378. https://doi.org/10.1080/08850607.2019.1565276

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior, 69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems, 21*(0). https://doi.org/10.3127/ajis.v21i0.1697

McCrae, R. R., & Costa, P. T., Jr. (1991). The NEO Personality Inventory: Using the Five-Factor Model in counseling. *Journal of Counseling & Development, 69*(4), 367-372. https://doi.org/10.1002/j.1556-6676.1991.tb01524.x

McCrae, R. R., & John, O. P. (1992). An introduction to the Five-Factor Model and its applications. *Journal of Personality, 60*(2), 175–215. https://doi.org/10.1111/j.1467-6494.1992.tb00970.x

McCrae, R. R. (2018). Defining traits. *The SAGE Handbook of Personality and Individual Differences: Volume I: The Science of Personality and Individual Differences,* 3-19.https://doi.org/10.4135/9781526451163.n1

McIntosh-Elkins, J., McRitchie, K., & Scoones, M. (2007). From the silent generation to Generation X, Y and Z: Strategies for managing the generation mix. *SIGUCCS*, 240–246. https://doi.org/10.1145/1294046.1294104

Mejias, R., & Balthazard, P. (2014). A model of information security awareness for assessing information security risk for emerging technologies. *Journal of Information Privacy and Security, 10*(160-185). https://doi.org/10.1080/15536548.2014.974407

Park, H. (H), Wiernik, B. M., Oh, I.-S., Gonzalez-Mulé, E., Ones, D. S., & Lee, Y. (2020). Meta-analytic five-factor model personality intercorrelations: Eeny, meeny, miney, moe, how, which, why, and where to go. *Journal of Applied Psychology.* https://doi.org/10.1037/apl0000476.supp

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017a). The Human Aspects of Information Security Questionnaire (HAIS-Q):

Two further validation studies. *Computers & Security, 66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram. (2014). Determining employee awareness using Human Aspects of Information Security Questionnaire (HAIS-Q). *Computer & Security, 42,* 165-176. https://doi.org/10.1016/j.cose.2013.12.003

Parry, E., & Urwin, P. (2011). Generational differences in work values: A review of theory and evidence. International *Journal of Management Reviews, 13*(1), 79–96. https://doi.org/10.1111/j.1468-2370.2010.00285.x

Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D., & McCormac, A. (2019). Matching training to individual learning styles improves information security awareness. *Information & Computer Security, 28*(1), 1–14. https://doi.org/10.1108/ICS-01-2019-0022

Pereira, S., Robinson, J., Peoples, H., Gutierrez, A., Majumder, M., McGuire, A., & Rothstein, M. (2017). Do privacy and security regulations need a status update? Perspectives from an intergeneration survey. *Plos One, 12*(9), 1-11. https://doi.org/10.1371/journal.pone.0184525

Pfleeger, S., & Caputo, D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597e611. https://doi.org/10.1016/j.cose.2011.12.010

Pilcher, Jane. (1994). Mannheim's sociology of generations: An undervalued legacy. *British Journal of Sociology 45,* 481–495.

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology, 63*, 539-569. https://doi-org.ezp.waldenulibrary.org/10.1146/annurev-psych-120710-100452

Popescu, A. (2019). The brief history of generation – defining the concept of generation. An analysis of literature review. *Journal of Comparative Research in Anthropology & Sociology, 10*(2), 15–30. https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=edsdoj&AN=edsdoj.50729b0ee86247e0ab2241b451608024&site=eds-live&scope=site

PricewaterhouseCoopers. (2014). *Why you should adopt the NIST cybersecurity framework*. Available at: www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the- nist.pdf.

Pricewaterhouse Coopers. (2015). *Key findings from the global state of information security survey 2016. Turnaround and transformation in cybersecurity.*

Rogler, L. H. (2002). Historical generations and psychology: The case of the Great Depression and World War II. *American psychologist, 57*(12), 1013.

Rummel, R. J. (1988). *Applied factor analysis.* Northwestern University Press.

Salvosa, H., & Hechanova, M. (2020). Generational differences and implicit leadership schemas in the Philippine workforce. *Leadership & Organization Development Journal, 42*(1), 47–60. https://doi.org/10.1108/LODJ-08-2018-0314

Sessa, V., Kabacoff, R., Deal, J., & Brown, H. (2007). Generational differences in leader values and leadership behavior. *The Psychologist Manger Journal,* 10(1), 47-74, http://doi:10.1080/10887150093366l2

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media Culture,* 1-6. Advance online publication. https://doi.org/10.1037/ppm0000247

Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A, 124*, 523–536. https://doi.org/10.1016/j.tra.2018.06.033

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. *Association for Information Systems,* (3443-3449).

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

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*. 104. 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Soto, C., & John, O. (2008). Ten facet scales for the Big Five Inventory: Convergence with NEO PI-R facets, self-peer agreement, and discriminant validity. Journal of Research in Personality, 43, 84-90. https://doi.org/10.1016/j.jrp.2008.10.002

SurveyMonkey. (2019). San Mateo, California, USA. https://www.surveymonkey.com

Sutin, A. R., & Terracciano, A. (2016). Five-factor model personality traits and the objective and subjective experience of body weight. *Journal of Personality, 84*(1), 102. https://doi.org/10.1111/jopy.12143

Thompson, N., McGill, T. J., & Wang, X. (2017). Security begins at home: Determinants of home computer and mobile device security behavior. *Computers & Security, 70*, 376–391. https://doi.org/10.1016/j.cose.2017.07.003

Tick, A. (2018). IT security as a special awareness at the analysis of the digital/e-learning acceptance strategies of the early z generation. *2018 IEEE 22nd International Conference on Intelligent Engineering Systems,* 45-50. https://doi.org/10.1109/INES.2018.8523964Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security, 79*, 68-79. https://doi.org/10.1016/j.cose.2018.08.007

VanderWeele, T. J. (2016). Mediation analysis: a practitioner's guide. *Annual review of public health, 37,* 17-32.

Verschoor, C. C. (2013, August 1). Ethical behavior differs among generations: a new study shows that the ethical behavior of younger workers differs from that of older generations. Business leaders should strengthen their ethics and compliance programs to address these differences. *Strategic Finance, 95*(2), 11. https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=edsgea&AN=edsgcl.340425211&site=eds-live&scope=site

Waldkirch, M. (2020). Non-family CEOs in family firms: Spotting gaps and challenging assumptions for a future research agenda. Journal of Family Business Strategy, 11(1). https://doi-org.ezp.waldenulibrary.org/10.1016/j.jfbs.2019.100305

Warner, R. (2013). Applied statics: from bivariate through multivariate techniques. *SAGE Publications.*

Weber, R., & Horn, B. (2017). Breaking bad security vulnerabilities. *Journal of Financial Service Professionals, 71*(1), 50-54. https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=bth&AN=120347240&site=eds-live&scope=site

Westen, D., & Rosenthal, R. (2003). Quantifying construct validity: two simple measures. *Journal of Personality and Social Psychology, 84*(3), 608.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 3-7.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 88. https://doi.org/10.1016/j.cose.2019.101640

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. IMIS Quarterly, *37(1),* 1-20. doi:10.25300/MISQ/2013/37.1.01

Zimmermann, V., & Renaud, K. (2019). Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. *International Journal of Human - Computer Studies*, *131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.0

Appendix A: Survey

Demographics:
What is your age?
18-85 with a drop down choice

Gender:
Use drop-down choice (s)
Female, male, self-described, prefer to not answer

Educational background:
HS, Associate Degree, Bachelor Degree, Master Degree or higher, other, Prefer to not answer;

Current employment:
Full-time, part-time, not employed, other, prefer to not answer;

Information Security Awareness:
This section will measure your security awareness. Respond using a Likert scale ranging from "Strongly disagree" to "Strongly agree"

The next set of questions refer to your use of work computers: (1) your knowledge of computer use guidelines, (2) your attitude towards the guidelines of computer use, (3) Your behavior while using a work computer (Parsons et al., 2007).

Focus area: Password Management		Knowledge	Attitude	Behavior
1	Using the same password	It's acceptable to use my social media passwords on my work accounts.	It's safe to use the same password for social media and work accounts.	I use a different password for my social media and work accounts
2	Sharing passwords	I am allowed to share my work passwords with colleagues.	It's a bad idea to share my work passwords, even if a colleague asks for it.	I share my work passwords with colleagues.
3	Using a strong password	A mixture of letters, numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters.	I use a combination of letters, numbers and symbols in my work passwords.
	Focus area: Email use			
4	Clicking on links in emails from known senders	I am allowed to click on any links in emails from people I know.	It's always safe to click on links in emails from people I know.	I don't always click on links in emails just because they come from someone I know.
5	Clicking on links in emails from unknown senders	I am not permitted to click on a link in an email from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender.	If an email from an unknown sender looks interesting, I click on a link within it.
6	Opening attachments in emails from unknown senders	I am allowed to open email attachments from unknown senders,	It's risky to open an email attachment from an unknown sender.,	I don't open email attachments if the sender is unknown to me.

Focus Area: Internet use				
7	Downloading files	I am allowed to download any files onto my work computer if they help me to do my job	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done.
8	Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the internet at work, I visit any website that I want to.
9	Entering information online	I am allowed to enter any information on any website if it helps me do my job.	If it helps me to do my job, it doesn't matter what information I put on a website.	I assess the safety of websites before entering information.
	Focus Area: Social media use			
10	Social Media (SM) privacy settings	I must periodically review the privacy settings on my social medica accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings.
11	Considering consequences	I can't be fired for something I post on social media.	It doesn't matter if I post things on social media that I wouldn't normally say in public.	I don't post anything on social media before considering any negative consequences.
12	Posting about work	I can post what I want about work on social media.	It doesn't matter if I post certain information about my work on social media.	I post whatever I want about my work on social media.
Focus area: Information handling				
13	Physically securing mobile devices	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute.	When working in a public place, I leave my laptop unattended.
14	Sending sensitive information via Wi-fi	I am allowed to send sensitive work files via a public Wi-fi	It's risky to send sensitive work files using a public Wi-fi network. It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.
15	Shoulder surfing	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.
Focus area: Incident handling				
16	Disposing of sensitive print-outs	Sensitive printouts can be disposed of in the same way as non-sensitive ones.	Disposing of sensitive printouts by putting them in a rubbish bin is safe.	When sensitive printouts need to be disposed of, I ensure that they are shredded or destroyed.

17	Inserting removable media	If I find a USB stick in a public place, I shouldn't plug it into my work computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer.	I wouldn't plug a USB stick found in a public place into my work computer.
18	Leaving sensitive material	I am allowed to leave print outs containing sensitive information on my desk overnight.	It's risky to leave print outs that contain sensitive information on my desk overnight.	I leave print outs that contain sensitive information on my desk when I'm not there.
Focus area: Incident reporting				
19	Reporting suspicious behavior	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen.	If I saw someone acting suspiciously in my workplace, I would do something about it.
20	Ignoring poor security behavior by colleagues	I must not ignore poor security behavior by my colleagues.	Nothing bad can happen if I ignore poor security behavior by a colleague.	If I noticed my colleague ignoring security rules, I wouldn't take any action.
21	Reporting all incidents	It's optional to report security incidents.	It's risky to ignore security incidents, even if I think they're not significant.	If I noticed a security incident, I would report it.

Personality Traits

Please respond whether you agree strongly, agree a little, neutral or neither agree nor disagree, disagree a little, disagree strongly;

1 Disagree Strongly	2 Disagree a little	3 Neither agree nor disagree	4 Agree a little	5 Agree strongly

Answer the following questions

1.		Is talkative	23.		Tends to be lazy
2.		Tends to find fault with others	24.		Is emotionally stable, not easily upset
3.		Does a thorough job	25.		Is inventive
4.		Is depressed, blue	26.		Has an assertive personality
5.		Is original, comes up with new ideas	27.		Can be cold and aloof
6.		Is reserved	28.		Perseveres until the task is finished
7.		Is helpful and unselfish with others	29.		Can be moody
8.		Can be somewhat careless	30.		Values artistic, aesthetic experiences
9.		Is relaxed, handles stress well	31.		Is sometimes shy, inhibited
10.		Is curious about many different things	32.		Is considerate and kind to almost everyone
11.		Is full of energy	33.		Does things efficiently
12.		Starts quarrels with others	34.		Remains calm in tense situations
13.		Is a reliable worker	35.		Prefers work that is routine
14.		Can be tense	36.		Is outgoing, sociable
15.		Is ingenious, a deep thinker	37.		Is sometimes rude to others
16.		Generates a lot of enthusiasm	38.		Makes plans and follows through with them
17.		Ends to be disorganized	39.		Gets nervous easily
18.		Tends to be disorganized	40.		Likes to reflect, play with ideas
19.		Worries a lot	41.		Has few artistic interests
20.		Has an active imagination	42.		Likes to cooperate with others
21.		Tends to be quiet	43.		Is easily distracted
22.		Is generally trusting	44.		Is sophisticated in art, music, or literature