

**GENERATIONAL DIFFERENCES IN THE FACTORS AFFECTING  
ORGANIZATIONAL CYBER SECURITY AWARENESS:  
A QUANTITATIVE STUDY**

by

Bruce Redekop

for

ANDREW BORCHERS, DBA, Faculty Mentor

WILLIAM J. McKIBBIN, PhD, Committee Member

KENNETH GRANBERRY, D.I.B.A., Committee Member

Barbara Butt Williams, PhD, Dean, School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Business Administration

Capella University

March 2016

© Bruce D. Redekop, 2016

## **Abstract**

The importance of Information Technology (IT) and Information Systems (IS) security is evident from the abundance of research conducted on the topic and from organizational expenditures ensuring the safeguarding of organizations' information systems and data holdings. Additionally, there exists significant research studying generations, the differences amongst generational cohorts, and the multigenerational workplace. The purpose of this study is to examine the nuances of the multigenerational workplace against the four factors affecting perceived security awareness levels depending on the generational cohort of the end user. Researchers have frequently referred to end users as being the weakest links in cyber security, and have observed that the most frequent types of security violations are non-malicious in nature. End user behavior or bad habits are detrimental to the security of organizational information systems regardless of the technological solutions put in place by network engineers and managers. Three generational cohorts, the Baby Boomers, Generation X, and Millennials, compose today's multigenerational workplace. Each cohort possesses unique habits, values, motivational factors, beliefs, and perceptions of the value of IT systems. By examining these differences and determining the factors that have the greatest influence on cyber security in each cohort, organizations can tailor their cyber security training and awareness efforts to the end users' generational cohort, thereby increasing compliance with organizational cyber security policies and their cyber security posture. The results of this study indicate that each generational cohort is influenced differently by the four factors that affect its members' perceived security awareness level. Given the characteristics of the three generational cohorts, the factor having the most influence on perceived security awareness relates to the generational cohorts' different attitudes, habits, and beliefs. Since each cohort possesses a factor that most influences its

members' security awareness, all four factors need to be considered by both executives and IT/IS specialists alike, as these factors are symbiotic in nature. While one factor is dominant in each cohort's level of security awareness, organizations will be best served by capitalizing on the factor most influencing positive security awareness while incorporating all four factors to contribute holistically to the creation of well-informed end users.

## **Dedication**

This dissertation is dedicated to my parents, David and Connie Redekop, and to my wife, Tonya Redekop. My parents instilled a “never give up” attitude in me early in life, a stance that helped me see this through to the end. Tonya’s encouragement, support, and staunch tolerance of the “never give up” attitude kept me steadfast throughout this exciting journey.

## **Acknowledgments**

Throughout my studies, there have been people who have encouraged me and supported my efforts, and the sum of their encouragement and support has helped me through challenging times. Special thanks to my mentor, Dr. Andrew Borchers, who was there from the beginning, providing me with valuable input throughout the dissertation process. Dr. McKibbin and Dr. Granberry provided valuable insights that forced me to add depth to my thought process and to re-examine concepts.

There are a few people who likely have no idea of the impact their supportive words have had on helping me remain confident and motivated. These include my long-time friend Erick Schibler, who always asked how I was progressing in my studies, and Jim Cheston, affectionately known as "Neighbor Jim," who was interested in my progress and requested a copy of the dissertation before it was even finished! I thank them all for their encouragement. Most of all, I wish to acknowledge members of the Silent and Baby Boomer generations. Their continual desire to open and forward emails containing jokes and attachments from unknown sources has always puzzled me, planting the idea of this dissertation in my mind.

Acknowledgments.....	iv
List of Tables .....	ix
List of Figures.....	xi
CHAPTER 1. INTRODUCTION .....	1
Introduction to the Problem .....	1
Background of the Study .....	2
Problem Statement.....	4
Purpose of the Study .....	5
Rationale .....	6
Research Questions.....	6
Significance of the Study .....	7
Definition of Terms.....	7
Assumptions and Limitations .....	8
Theoretical Framework.....	8
Organization of the Remainder of the Study .....	9
CHAPTER 2. LITERATURE REVIEW .....	10
Generational Considerations.....	10
Generations Defined .....	11
Silent Generation (1925 – 1945).....	13
Baby Boom Generation (1946 – 1964).....	15
Generation X (1965 – 1980) .....	18
Millennials (1981 – 2000).....	20
Motivational Factors and Values .....	22

Ethical Beliefs and Work Habits.....	24
Boomers: Habits and beliefs. ....	26
Generation X: Habits and beliefs.....	28
Millennials: Habits and beliefs. ....	30
Generational Perspective on IT Purpose and Functionality.....	32
Preferred Training Methods.....	36
Cyber Security Awareness and Governance.....	40
Cyber Security Awareness Training.....	44
Factors Influencing the Perceived Security Awareness Level of End Users.....	46
Internal IT Factors.....	46
Internal Management Factors .....	47
External Factors .....	48
Inherent Factors .....	48
CHAPTER 3. METHODOLOGY .....	50
Research Design.....	50
Sample.....	51
Survey Instrument.....	52
Hypotheses .....	52
Data Collection .....	55
Data Analysis .....	56
Validity and Reliability.....	56
Ethical Considerations .....	57
CHAPTER 4. RESULTS.....	58



Sample and Setting .....	59
Survey Instrument.....	60
Demographics .....	60
Security Awareness.....	64
Internal IT Factors.....	65
Internal Management Factors .....	66
External Factors .....	66
Inherent Factors .....	67
Perceived Security Awareness Level.....	68
Hypothesis Results.....	69
Hypothesis 1: Internal IT Factors (security awareness training) .....	70
Hypothesis 2: Internal Management Factors .....	76
Hypothesis 3: External Factors .....	82
Hypothesis 4: Inherent Factors .....	88
Summary .....	94
CHAPTER 5. DISCUSSION, IMPLICATIONS, AND RECOMMENDATIONS .....	95
Summary .....	95
Research Questions.....	95
Discussion.....	96
Influencing Factors and their Significance in Business .....	97
Primary Motivating Factors by Generational Cohort .....	101
Baby Boomer .....	102
Generation X.....	103

Millennials .....	104
Recommendations .....	105
Further Research .....	107
References .....	109
APPENDIX A – Statistical Tests.....	115
Reliability Statistics .....	115
Chronbach’s Alpha .....	115
Descriptive Statistics.....	116
Internal IT Factors.....	116
Internal Management Factors .....	120
External Factors .....	124
Inherent Factors .....	128
Perceived Security Awareness Level.....	132
APPENDIX B – Survey Instrument .....	136

## **List of Tables**

Table 1: Characteristics of the Silent Generation .....	14
Table 2: Characteristics of the Baby Boomer Generation .....	17
Table 3: Characteristics of Generation X.....	19
Table 4: Characteristics of Millennials .....	21
Table 5: Frequency Table - Generational Cohorts.....	61
Table 6: Frequency Table - Gender of participant.....	62
Table 7: Frequency Table - Employment/Student status .....	62
Table 8: Frequency table - Years of Employment/at school.....	63
Table 9: Frequency table - Level of education .....	63
Table 10: Frequency table - Percentage of day spend on the computer .....	64
Table 11: Pearson Correlation - Internal IT Factors (Baby Boomer) .....	71
Table 12: ANOVA - Internal IT Factors (Baby Boomer).....	72
Table 13: Pearson Correlation - Internal IT Factors (Generation X).....	73
Table 14: ANOVA - Internal IT Factors (Generation X) .....	74
Table 15: Pearson Correlation - Internal IT Factors (Millennial).....	75
Table 16: ANOVA - Internal IT Factors (Millennial) .....	76
Table 17: Pearson Correlation - Internal Management Factors (Baby Boomer) .....	77
Table 18: ANOVA - Internal Management Factors (Baby Boomer) .....	78
Table 19: Pearson Correlation - Internal Management Factors (Generation X).....	79
Table 20: ANOVA - Internal Management Factors (Generation X) .....	80
Table 21: Pearson Correlation - Internal Management Factors (Millennial).....	81
Table 22: ANOVA - Internal Management Factors (Millennial) .....	82

Table 23: Pearson Correlation - External Factors (Baby Boomer).....	83
Table 24: ANOVA - External Factors (Baby Boomer) .....	84
Table 25: Pearson Correlation - External Factors (Generation X) .....	85
Table 26: ANOVA - External Factors (Generation X).....	86
Table 27: Pearson Correlation - External Factors (Millennial) .....	87
Table 28: ANOVA - External Factors (Millennial).....	88
Table 29: Pearson Correlation - Inherent Factors (Baby Boomer).....	89
Table 30: ANOVA - Inherent Factors (Baby Boomer) .....	90
Table 31: Pearson Correlation - Inherent Factors (Generation X).....	91
Table 32: ANOVA - Inherent Factors (Generation X).....	92
Table 33: Pearson Correlation - Inherent Factors (Millennial).....	93
Table 34: ANOVA - Inherent Factors (Millennial) .....	94
Table A1: Chronbach's Alpha – Internal IT Factors .....	115
Table A2: Chronbach's Alpha – Internal Management Factors .....	115
Table A3: Chronbach's Alpha – External Factors .....	115
Table A4: Chronbach's Alpha – Inherent Factors .....	115
Table A5: Chronbach's Alpha – Perceived Security Awareness Level .....	115

## List of Figures

Figure 1: Theoretical Framework .....	9
Figure 2: Scatter plot - Internal IT Factors (Baby Boomer) .....	71
Figure 3: Scatter plot - Internal IT Factors (Generation X) .....	73
Figure 4: Scatter plot - Internal IT Factors (Millennial) .....	75
Figure 5: Scatter plot - Internal Management Factors (Baby Boomer) .....	77
Figure 6: Scatter plot - Internal Management Factors (Generation X) .....	79
Figure 7: Scatter plot - Internal Management Factors (Millennial) .....	81
Figure 8: Scatter plot - External Factors (Baby Boomer) .....	83
Figure 9: Scatter plot - External Factors (Generation X) .....	85
Figure 10: Scatter plot - External Factors (Millennial) .....	87
Figure 11: Scatter plot - Inherent Factors (Baby Boomer) .....	89
Figure 12: Scatter plot - Inherent Factors (Generation X) .....	91
Figure 13: Scatter plot - Inherent Factors (Millennial) .....	93
Figure A1: QQ Plot - Internal IT Factors (All Generations) .....	116
Figure A2: Histogram - Internal IT Factors (All Generations) .....	116
Figure A3: QQ Plot - Internal IT Factors (Baby Boomers) .....	117
Figure A4: Histogram - Internal IT Factors (Baby Boomers) .....	117
Figure A5: QQ Plot - Internal IT Factors (Generation X) .....	118
Figure A6: Histogram - Internal IT Factors (Generation X) .....	118
Figure A7: QQ Plot - Internal IT Factors (Millennials) .....	119
Figure A8: Histogram - Internal IT Factors (Millennials) .....	119
Figure A9: QQ Plot - Internal Management Factors (All Generations) .....	120

Figure A10: Histogram - Internal Management Factors (All Generations).....	120
Figure A11: QQ Plot - Internal Management Factors (Baby Boomers).....	121
Figure A12: Histogram - Internal Management Factors (Baby Boomers) .....	121
Figure A13: QQ Plot - Internal Management (Generation X).....	122
Figure A14: Histogram - Internal Management Factors (Generation X) .....	122
Figure A15: QQ Plot - Internal Management (Millennials) .....	123
Figure A16: Histogram - Internal Management Factors (Millennials).....	123
Figure A17: QQ Plot - External Factors (All Generations) .....	124
Figure A18: Histogram - External Factors (All Generations) .....	124
Figure A19: QQ Plot - External Factors (Baby Boomers).....	125
Figure A20: Histogram - External Factors (Baby Boomers).....	125
Figure A21: QQ Plot - External Factors (Generation X).....	126
Figure A22: Histogram - External Factors (Generation X) .....	126
Figure A23: QQ Plot - External Factors (Millennials) .....	127
Figure A24: Histogram - External Factors (Millennials).....	127
Figure A25: QQ Plot - Inherent Factors (All Generations) .....	128
Figure A26: Histogram - Inherent Factors (All Generations).....	128
Figure A27: QQ Plot - Inherent Factors (Baby Boomers).....	129
Figure A28: Histogram - Inherent Factors (Baby Boomers) .....	129
Figure A29: QQ Plot - Inherent Factors (Generation X) .....	130
Figure A30: Histogram - Inherent Factors (Generation X) .....	130
Figure A31: QQ Plot - Inherent Factors (Millennials).....	131
Figure A32: Histogram - Inherent Factors (Millennials).....	131

Figure A33: QQ Plot – Perceived Security Awareness Level (All Generations) .....	132
Figure A34: Histogram - Perceived Security Awareness Level (All Generations) .....	132
Figure A35: QQ Plot - Perceived Security Awareness Level (Baby Boomers) .....	133
Figure A36: Histogram - Perceived Security Awareness Level (Baby Boomers).....	133
Figure A37: QQ Plot - Perceived Security Awareness Level (Generation X) .....	134
Figure A38: Histogram - Perceived Security Awareness Level (Generation X).....	134
Figure A39: QQ Plot - Perceived Security Awareness Level (Millennials) .....	135
Figure A40: Histogram - Perceived Security Awareness Level (Millennials) .....	135

## **CHAPTER 1. INTRODUCTION**

### **Introduction to the Problem**

Companies are increasingly dependent on information systems (IS), information technology (IT), and electronic data, collectively known as cyber systems, in the conduct of their business. This dependency demands that cyber systems be readily available for employees within the organizations; the availability of such systems increases the risk of security breaches that can be either malicious or non-malicious. Organizations spend a notable portion of their resources securing their cyber systems. Guo, Yuan, Archer, and Connelly (2011) claimed that, regardless of the complexity or intricacy of organizational defensive cyber security systems, the intended security can be circumvented through either the malicious or the non-malicious actions of insiders. The prevention of malicious attacks is challenging and, typically, organizations rely on technological solutions for this. Non-malicious security violations (NMSV) are security infractions that can be mitigated through effective training in cyber security and information assurance (IA). Effectively training and educating end users enhances an organization's cyber security posture with respect to this problematic security issue (Guo et al., 2011).

The first decade of the new millennium marked the first time ever that four distinct generational cohorts, the Silent, Baby Boomer (Boomer), Generation X (Gen X), and Millennial generations, concurrently occupied the workforce (Cekada, 2012; Houck, 2011). Each of these generations carries its own distinct habits, ethics, and values, thereby contributing uniquely to the cyber security risks in an organization. By examining the differences each generation possesses, cyber security managers will better understand how to develop effective cyber security policy awareness in the multigenerational workforce.



Cyber security has become a significant security issue for both business and government. In May 2009, the White House established an office that was instrumental in the development, employment, and integration of measures designed to protect the cyber infrastructure of the United States (Asner & Kleyna, 2009). The purpose of the office was to enhance cyber security awareness through the development of training and awareness programs. Policy compliance is a significant challenge and, in order to increase compliance, the establishment of cyber security awareness programs is essential. Compliance adherence can be solicited through a variety of methods that include end user training, control mechanisms, and incentivized rewards for compliance (Chen, Ramamurthy, & Wen, 2012; Fehr & Schmidt, 2007). One of the challenges that organizations face today is the difficulty of training a multigenerational workforce (Cekada, 2012). Incentives, motivation, training approaches, and control mechanisms are significantly different for each generational cohort in the multigenerational workforce, and it is no longer suitable to use one single methodology. Organizations need to adapt their cyber security training approach to effectively educate the multigenerational workforce and prevent NMSVs.

### **Background of the Study**

Chen, Ramamurthy, and Wen (2012) studied how carelessness on the part of end users, malicious and non-malicious infractions, and insider incidents can all compromise the security efforts established by organizations. According to Decker (2008), an essential component in the assurance of compliance is for employees to follow established organizational security policies, and it is only through security awareness training that compliance can be achieved. The costs involved in ensuring policy compliance pose a challenge for cyber security staff and management at all levels, who must perform a careful balancing act between financial resources and the level of security expected and required by the organization (Richardson & Director,

2008). Executives who understand the multigenerational workforce dynamic will be better able to minimize costs while maximizing security.

Guo, Yuan, Archer, and Connelly (2011) explored the concept of NMSV, and more precisely the motivations causing end users to act carelessly regarding corporate cyber security directives. Organizations may possess a robust and comprehensive cyber security policy, yet the policy will not guarantee end user compliance. Guo et al. (2011) outlined four characteristics common to end users engaged in non-malicious security violations. According to Guo et al., such violations are:

- Intentional – End users make conscious decisions to breach the organization’s cyber security policy.
- Self-benefiting without malicious intent – End users attempt to help themselves by saving time and effort that would be required if they followed the rules. These users have no malicious intention to harm the cyber security infrastructure and do not engage in unethical behaviors that would be detrimental to the organization.
- Voluntary – End users engaging in this type of behavior do so voluntarily; they do not feel the need to follow the rules that have been set out by the organization.
- Possible causes of damage or security risk – Not only do users engaging in NMSVs break rules, but their actions can cause damage to organizational IS infrastructure and put the organization’s intellectual property at risk.

Guo et al. (2011) went on to explain that NMSVs are not illegal, nor are they malicious compared to illegal actions such as computer abuse, IS misuse, security contravention, unethical use, and behavior that disregards cyber security policy. While NMSVs are not illegal, the consequences are significant and their effect on organizations is similar if not identical to

criminal or unlawful activity. NMSVs need to be mitigated using cyber security education and training tailored to the generational cohort of the employee, thereby increasing compliance and preventing corporate losses.

A multigenerational workforce populates today's workplace. As almost all members of the Silent Generation have now retired, the workforce is now comprised almost entirely of the Baby Boomer Generation, Generation X, and the Millennial Generation (Howe & Strauss, 2007; Simons, 2010). The management of a multigenerational workforce needs to develop and provide a dynamic, generationally driven security awareness program. Each generation, Boomer, Gen X, and Millennial, will respond to different training approaches (Cekada, 2012). Not only are training approaches distinct for the different generations (Reeves & Oh, 2008), but the value placed on cyber security will be different for each generational cohort based on their perception of IT. In order to minimize NMSVs in the multigenerational workforce, it is necessary to examine the generations themselves: their values, habits, motivational factors, and perspectives on IT systems.

### **Problem Statement**

Organizations rely heavily on the integrity of their cyber systems to conduct their operations, and they face increasing costs, through loss of revenue or reputation, from end users who do not adhere to organizational policies. Organizations of all sizes are affected by NMSVs, and small businesses are the most vulnerable as they do not possess the resources required to protect themselves as diligently as larger firms can (Pullen, 2013). Organizations attempt to ensure adherence to their security policies through hardware, software, and policy measures, yet the weakest link in the cyber security chain remains the end user. Chen et al. (2012) stated that

employees tend to resort to their habitual use of the organizational IT infrastructure and, as a result, tend to ignore established policies.

Evidence in academic literature substantiates the importance of the development of effective cyber security policies (Dutta & McCrohan, 2002; Hu, Dinev, Hart, & Cooke, 2012; Puhakainen & Siponen, 2010). Policies are rendered ineffective when employees using cyber systems are unaware of the policies and the rationale for adherence. Violations of this type are considered NMSVs (Guo et al., 2011), and may indicate a poorly designed cyber security policy. More often than not, the organization has an ineffective cyber security training and awareness program. Organizations developing awareness training should avoid a “one size fits all” training plan, and should instead take into account the training needs of their multigenerational workforce (Reeves & Oh, 2008). Training and delivery methodologies that take multigenerational considerations into account will resonate with the multigenerational workforce, increasing policy compliance (Puhakainen & Siponen, 2010). There are gaps in research on the relationship between the multigenerational workforce and cyber security awareness and whether policy violations can be attributed to ineffective training of the multigenerational workforce.

### **Purpose of the Study**

Using Decker’s (2008) security behavior factors, this study will use non-experimental quantitative methods to investigate the influence of a multigenerational workforce on the security awareness of end users. NMSVs by end users account for over fifty percent of security breaches; this study will examine the effects of the multigenerational workforce on such breaches (Holbert, 2013; Siponen & Vance, 2010). Decker (2008) studied end users’ security behavior based on internal IT, internal management, external, and inherent factors. End users’ security awareness

was measured against these four factors to determine which factor had the most significant effect on the perceived level of security awareness of end users.

Cyber security policy violations negatively affect organizations, requiring them to adopt methodologies to educate the multigenerational workforce to create a corporate culture of cyber security. The intent of this study is to increase the body of knowledge regarding best practices and practical awareness training methodologies that can foster positive change in a multigenerational workforce. While existing research examines the factors affecting end users' security awareness, no research can be found that examines the cyber security awareness of a multigenerational workforce. Increasing compliance with organizational cyber security policies through effective awareness training can minimize corporate losses in terms of both data and financial and intellectual property.

### **Rationale**

This examination will further the studies conducted by Decker (2008) and Holbert (2013). Decker (2008) analyzed the significance of the contributions of internal IT, internal management, external, and inherent factors to the computer security awareness of end users in institutions of higher learning. Holbert (2013) used Decker's (2008) four factors to determine which had the greatest influence on the security awareness level of end users. This study will use Decker's (2008) four factors that influence security awareness, measuring each generational cohort against these four factors to see how each cohort is different.

### **Research Questions**

This research seeks to understand how the generational cohort of employees can affect their awareness of corporate cyber security policies. The intent of this research is to answer the following questions:

RQ1: What is the relationship between internal IT Factors and the cyber security awareness of end users from each generational cohort?

RQ2: What is the relationship between internal management factors and the cyber security awareness of end users from each generational cohort?

RQ3: What is the relationship between external factors and the cyber security awareness of end users from each generational cohort?

RQ4: What is the relationship between inherent factors and the cyber security awareness of end users from each generational cohort?

### **Significance of the Study**

By analyzing Decker's (2008) factors that influence security awareness in end users, organizations are able to better ensure their cyber security. The research conducted by Decker (2008) and Holbert (2013) clearly indicated the relationship of Decker's factors to the security awareness of end users. Through the implementation of proper security awareness training, organizations are able to minimize risks by changing both the corporate culture and end user behavior. Research has shown that end users who are not trained in security awareness pose a substantial risk to their organizations (Decker, 2008; Harris, 2010; Holbert, 2013; McCrohan, Engel, & Harvey, 2010).

### **Definition of Terms**

*Cyber* – The collection of Information Systems and Information Technology as well as the medium through which IT and IS are transported.

*Information Systems (IS)* – The collection of hardware, software, data, and people that deliver knowledge, information, and digital products.

*Information Technology (IT)* – The systems, composed of computers and telecommunications devices and networks, that store, retrieve, and send information.

*Information Systems Security Policy* – An organizational policy document that outlines how the organization plans to protect its IT and IS assets.

*Multigenerational workforce* – A group of people from the Baby Boomer, Generation X, and Millennial generations in either an academic or business work setting.

*Non-malicious Security Violation (NMSV)* – the non-malicious non-adherence of end users of an Information System (IS) to organizational security policies regarding the usage of the IT infrastructure (Guo et al., 2011).

### **Assumptions and Limitations**

Assumptions:

1. End users will be able to access and complete the survey over the Internet.
2. Participants can complete the survey honestly without fear of retaliation.
3. Respondents will come from varied backgrounds.

Limitations: The survey questions will not be made available to the Silent Generation or to anyone under the age of 21.

### **Theoretical Framework**

The research will examine Decker's (2008) factors that affect the security awareness of end users. These include security awareness training or internal IT factors, management commitment or internal management factors, and external and inherent factors. These four factors will be examined through a generational lens to better understand how each generational cohort views the importance of each factor and how this influences organizational security

awareness. While Decker's (2008) factors will be used in the survey instrument, generational traits will define how each generation views the factors outlined by Decker.

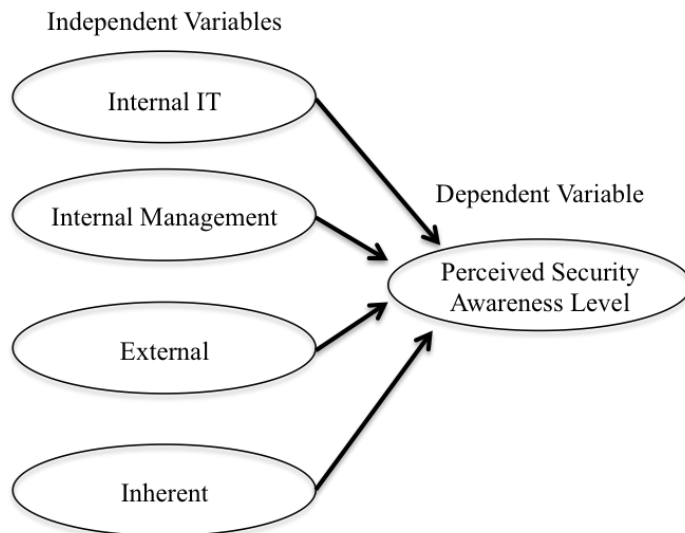


Figure 1: Theoretical Framework

### **Organization of the Remainder of the Study**

This study is organized into the five chapters required by Capella University. Chapter 1 was an introduction to the study and Chapter 2 will be a review of the literature on the generations, what drives them, and their habits and beliefs. It will examine the different generations' views of IT in the workplace and their preferred training methods. It will also study IS security training and IS security policy compliance. Chapter 3 will review the methodology used in the research conducted and the research design.

The findings of the study will be summarized and analyzed in Chapter 4, leading to Chapter 5, where conclusions from the study will be drawn. Additionally, there will be a summary and discussion of the results, implications for theory and practice, and recommendations.



## **CHAPTER 2. LITERATURE REVIEW**

While there is research on generational trends and definitions and significant research on IS security policy adherence, there is limited information or research regarding the influence of generations and their perceptions on IS security policy adherence. Much research has been dedicated to the multigenerational workplace and workforce and to the impact of this multigenerational phenomenon. This literature addresses how attitudes, ethics, and views influence behaviors in different cohorts within the multigenerational workforce. With such an understanding of how the different generations function, it will be possible to examine the impact of the multigenerational workforce on an organization's IS security.

This chapter will first look closely at the attributes of the different generational cohorts to better understand the motivating factors of each generational cohort and how they relate to internal IT, internal management, external, and inherent factors. Only through an examination of the differences and similarities of the generational cohorts will it be apparent how they relate to Decker's four factors. The latter portion of the chapter will examine cyber security awareness, governance, and training.

### **Generational Considerations**

The current landscape of the workforce is poised to change as the Generation X and Millennial generations prepare to assume command of leadership positions left behind by retiring Baby Boomers. McCrindle and Wolfinger (2010) claimed that this generational dynamic has proven to be one of the most significant changes experienced in the workplace in the twenty-first century. Ludwick (2007) estimated that by the year 2020 approximately 20 percent of the workforce, which equates to 25 million workers, will be ready to retire. Ludwick (2007) also predicted that by the year 2008, Generation X would assume the dominant space in the

workforce. This prediction did not come to fruition because of the economic downturn that began in 2008. Over a short period of two years, Baby Boomers saw a significant reduction in the retirement savings they had been counting on for retirement. In some cases, Baby Boomers lost almost all of their savings, requiring them to remain in the workforce well past 2008.

### **Generations Defined**

Throughout the literature relating to generational issues, it is common to find a variety of terms used for similar generations. This makes it difficult to describe the term “generation” as there is no clear, conclusive description of the term and as demographers such as Howe and Strauss describe the generations using different names and timelines. McCrindle and Wolfinger (2010) stated that the most likely explanation for this difficulty is that the concept of labeling a generation did not exist before the Baby Boomer generation. Traditionally, a generation has been defined in terms of the time span between the birth of parents and the birth of their children. Howe and Strauss (1991) defined a generation in their seminal work as “a group of people who share a time and space in history that lends them a collective persona.” Davis, Pawlowski, and Houston (2006) made it clear that, in generational research, it is important to clearly define the generations of interest to accurately compare the results of the study.

Smola and Sutton (2002) identified generational groups as groups of individuals born within particular periods in time within which they not only share social and historical experiences or events but also ethics, values, attitudes, and shared language or slang. Mannheim (1952) explained that generations are shared experiences of a historical nature and that a generational cohort can be defined as a group born in a specific period and sharing a unique character that is a function of their common age location in history.

Howe and Strauss (1991) described generations as a biological function wherein a generation is defined by life span and average life expectancy. In the nineteenth century, social and historical variables became factors that influenced the bounds of a particular generation. Currently, the concept of generations being chronologically and biologically defined is becoming outdated. Generations such as the Millennials are now starting to be identified with technological change, not simply biological or chronological timelines. McCrindle and Wolfinger (2010) postulated that the previous, biologically driven methodology for determining a generational cohort is not relevant with newer generations. They stated that while these traditional definitions served people well in the past, these definitions are becoming meaningless due to the technological changes that are being introduced. The rapid proliferation and advancement of cyber systems are dictating that two decades is too long, causing McCrindle and Wolfinger (2010) to believe that generations of the future will have a shorter chronological duration as generational cohorts will be bound by technological timelines.

Depending on the author(s) being referenced, the labels applied to the different generations from the past century vary. People born before 1946 are known as *Builders*, *The GI Generation*, *the Silent Generation*, and *Traditionalists*. The generation born to the aforementioned generation is commonly known as *the Baby Boom Generation*, *Baby Boomers*, and *Boomers*. The next generation is called *Generation X*, *Gen X*, *Echo Boomers*, *Xers*, or *Generation 13*. The last generation of this past century is known as *Generation Y*, *Gen Y*, *Millennials*, *Digital Natives*, or the *Net Gen* (Cekada, 2012; Lippincott, 2010; McCrindle & Wolfinger, 2010; Simons, 2010; Verschoor, 2013; Wilson, 2009).

In order to remain consistent and for the purposes of this study, the following generational nomenclature as outlined by Cekada (2012) will be used.

1. Silent Generation – born between 1925-1945 (Howe & Strauss, 1991).
2. Baby Boomer – born between 1946-1964 (McCrindle & Wolfinger, 2010).
3. Generation X – born between 1965-1980 (Cekada, 2012).
4. Millennials – born between 1981-2000 (Cekada, 2012).

### **Silent Generation (1925 – 1945)**

The Silent Generation is the generation that was born shortly after the Depression in the 1920s and throughout the Second World War. Their experiences included growing up in austere conditions that were a significant formative variable. They are seen as change-resistant conformists who possess a clear delineation between work and family life and tend to dress formally (Verschoor, 2013). The events that defined the lives of those in this generation are the Great Depression in the 1930s, the rise of communism, and World War II from 1939-1945.

This generation formed work ethics centered around loyalty, discipline, and knowledge (Cekada, 2012). Being loyal, members of this generation set aside their personal desires and formed groups to work collectively towards common goals for the good of their community or nation. They placed implicit trust in their leaders and their strong work ethic meant they willingly dedicated themselves to the long-term good of their employers or organizations (Cekada, 2012). Other generations may classify the Silent Generation as inflexible or overcautious, slow to adapt to change, and not technologically knowledgeable.

The generational boundaries of this generational cohort are defined primarily by the generations before and after them. This generation was too late to enter World War II and, while they have memories of the war, they did not experience it in the trenches as the generation before them had. The result of this was that many Silents joined organizations such as the Peace Corps in an attempt to make the world a better place (Bell, 2008). The Silent Generation thrives on

being needed, enjoys being able to mentor others, and does not crave power; it embraces fairness and transparency and, as such, it is easy to understand why virtually all modern civil rights leaders are from this generation (Bell, 2008).

According to the United States Census Bureau, as of 2010, the Silent Generation accounted for only five percent of the total United States labor force. Therefore, while the Silent Generation is discussed in this study, it is not included in the research.

Table 1: Characteristics of the Silent Generation

Author(s)	Characteristics of the Silent Generation (Summary)
Cekada (2012)	Known as the Silent Generation, Traditionalists, or Veterans; born 1933 to 1945; grew up following the Great Depression; experienced significant economic hardships that formed their need to ensure their own financial security or self-developed wealth; self-sacrificing; display a work ethic that is loyal, disciplined, and knowledgeable; long-term loyalty to company.
Verschoor (2013)	Known as Traditionalists; conformists who resist change; disciplined and pragmatic; separation of work and family life; dress formally.
McCrindle and Wolfinger (2010)	Known as the Builders and the Greatest Generation; born 1925-1945; born during a crisis period: Great Depression and World War II; started families during the post-WWII boom; currently the senior generation.
Wilson (2009)	Known as Traditionalists; born 1900-1945; main trait is loyalty; patriotic; chain of command is essential; other generations view them as inflexible, overcautious, not technologically savvy, even slow.
Al-Asfour and Lettau (2014)	Known as Veterans; born 1922-1943; dedicated and hard working; respect for authority; defined by the Great Depression and World War II, Charles Lindbergh and FDR.
Howe and Strauss (2007)	Known as the Silent Generation; born 1925-1942; Great Depression and World War II; came of age too late for WWII and too early to be youthful “free spirits”; risk-averse; early marriage; willing to climb the corporate ladder to ensure success; conformists accepting of institutional civic life and conventional culture of the GIs; leading civil rights leaders; antiwar leaders, feminists, and mentors; rose to political power during Watergate.

## **Baby Boom Generation (1946 – 1964)**

This generation was the post-World War II generation. It saw significant changes and is divided into two categories. Boomers who were born between 1946 and 1955 are classified as “older” and Boomers born between 1956 and 1964 are categorized as “younger” (Hicks & Block, 2014). The significant developments in this generation included the introduction of the television and the transistor radio. This generation grew up in a period of prosperity and wealth and had a distinct sense of entitlement (Hicks & Block, 2014). They consider themselves to belong to a special generation, the generation that embraced the Women’s Rights and Civil Rights movements (Simons, 2010). The period of affluence and economic prosperity in which the Boomers grew up was unprecedented. Baby Boomers had a tendency to embrace the suburban lifestyle and to form strong nuclear families that included stay-at-home mothers. As parents, Boomers demonstrated a self-sacrificing and hard-working work ethic (Cekada, 2012), fully expecting that they would have to “do the time” before they could make demands at work. The Boomer generation is likely the most studied generation to date. According to Simons (2010), the term “generation gap” was first introduced in the 1960s. This description explained the differences experienced between the Silent Generation and the Baby Boomers and what each generation could do to coexist in harmony.

Increasing wealth and the desire for social change are classic characteristics of this generation. Given the period in which they grew up, they were the wealthiest generation, and they were also the healthiest one (Simons, 2010). This all changed with the recession that started in 2008, interrupting the Boomers’ retirement plans and delaying their retirements. Boomers feel financially squeezed, as 40% exist paycheck to paycheck (Hicks & Block, 2014). This delay in their retirements has translated into their remaining in senior management positions

that are now unattainable by younger generations. While the Boomers await an economic upswing to allow their retirement savings to increase, the younger generations are growing impatient to assume positions they feel they should occupy. This tension at work compounds the multigenerational tension that is already simmering in the workplace (Wilson, 2009). In the early and mid 2000s, it was speculated that there would be a mass exodus of employees starting in 2007 as Baby Boomers left work to head into retirement (Ludwick, 2007). This, of course, never transpired due to the economic depression that started in 2008. Boomers decided to stay at work and wait for a resurgence of the economy so their retirement savings could increase.

A problem facing managers is that Boomers are becoming increasingly disengaged (Thielfoldt, 2014). According to the 2010 US Census, Boomers are the generation with the highest labor force participation at 38%. Thielfoldt (2014) claimed that Boomers are the least engaged generation and the most actively disengaged generation working today. They have postponed their retirements and are not likely to retire in the near future. Managers will need to find new, innovative ways to invigorate and motivate this generation that was previously known to be an optimistic, competitive, and workaholic generation (Al-Asfour & Lettau, 2014; Cekada, 2012; Verschoor, 2013; Wilson, 2009).

Table 2: Characteristics of the Baby Boomer Generation

Author(s)	Characteristics of the Baby Boomer Generation (Summary)
Simons (2010)	Known as the Baby Boomers or Boomers; born 1946-1964; inspired social change and were wealthy; healthiest generation; they consider themselves a special generation; they prefer centralized and institutionalized business and government; high regard for institutional information.
Cekada (2012)	Known as Baby Boomers; born 1946-1964; lost the opportunity to retire in the economic downturn of 2009; grew up with economic prosperity; strong nuclear families; stay-at-home moms; competitive and hard working; currently hold management positions; strong devotion to work; develop and follow rules.
Verschoor (2013)	Known as Boomers; self-centered, with a feeling of entitlement; workaholics, self-motivated, do not appreciate feedback.
McCrindle and Wolfinger (2010)	Known as Baby Boomers; born 1946-1964; high spenders in younger years; unraveling old-age crisis; born into the post-WWII boom; included several civil rights leaders in early adulthood.
Wilson (2009)	Known as Baby Boomers; born 1946-1964; optimistic generation that questions the status quo; intensely competitive and workaholic; viewed by other generations as self-centered micromanagers.
Al-Asfour and Lettau (2014)	Known as Baby Boomers; born 1946-1964; known for their optimism and for personal gratification and growth; dislike traditional hierarchy; prefer a collegial and consensual style.
Howe and Strauss (2007)	Known as Boom Generation; born 1943-1960; dubbed Dr. Spock babies due to the influence Dr. Spock's books had on rearing children; materialistic in post-war years; civil participation; questioned the status quo; suburbs and stay-at-home moms; Vietnam War protestors.



## **Generation X (1965 – 1980)**

Generation X, or Gen X as it is commonly referred to, is a prominent generational cohort that is viewed negatively by other generations as being lazy, skeptical, and cynical (Verschoor, 2013). This generation became the first generation to embrace the electronic age. Gen X was the first generation to see the introduction and mass production of personal computers, video games, home electronics, and cellular phones. Unlike the previous generation's family unit, the family unit in this generation suffered as it was subject to more single working parent families, making Generation X a generation of latchkey children (Cekada, 2012). This suffering of the family unit resulted in a distrust of institutions as well as of marriage and family.

While other generations view Gen X negatively, this generation does not accept this view. They feel they are a generation of practical, observant, and adaptable people due to the challenges they endured growing up (Howe & Strauss, 1991). This generation developed methods to overcome the challenges they faced. As youngsters, they watched the US military fail in Vietnam, and they witnessed the decline in ethical politics starting with the Watergate scandal and the rise in consumerism dominated by manufacturers in Japan and China. Industrial globalization took hold and the manufacturing segment of the United States declined in favor of cheaper goods from countries that possessed cheaper labor (Howe & Strauss, 1991). In 2012, this generation began to feel cheated out of what they felt was their rightful place in corporate America (Cekada, 2012). Due to the economic downturn of 2008, the Boomer Generation is not retiring en masse as expected. The result of this is that Generation X is unable to progress in their careers as they had expected.

Table 3: Characteristics of Generation X

Author(s)	Characteristics of Generation X (Summary)
Simons (2010)	Known as Generation X; born 1965-1976; Pragmatic and practical generation that is highly self-reliant and individualistic; tendency to reject rules; enjoy living life on the edge; an innate distrust of institutions; first generation to see the mass production of the PC, which has enabled their technological knowledge; They prefer being involved at work in a casual friendly workplace where they can learn; they appreciate freedom and flexibility at work.
Cekada (2012)	Known as Generation X; born 1965-1980; born into a new paradigm of working mothers and increased divorce, latchkey kids became the norm; an independent and adaptable generation; observed parents face job insecurity and layoffs and are therefore not loyal to organizations; able and willing to change jobs quickly to adapt to economy.
Verschoor (2013)	Known as Gen Xers; lazy, skeptical, and cynical; they question authority and desire a work-life balance and flexible schedule; they dress in the low end of business casual.
McCrindle and Wolfinger (2010)	Known as Generation X or Gen Xers; born 1965-1979; born during an awakening; spent early adult years pre-September 11, resulting in their living through the crisis stage of their midlife.
Wilson (2009)	Known as Generation X; born 1965-1980; Greater desire for independence; latchkey childhood, as both parents worked or they had single-parent homes; computer pioneers; the smallest generation; viewed by other generations as slackers cynical, or rude.
Al-Asfour and Lettau (2014)	Known as Generation X; born 1961-1980; embrace diversity, technically literate; prefer a fun, informal setting.
Howe and Strauss (2007)	Known as Generation X; born 1961-1981; grew up in an era of failing marriages and education; distrust of institutions, including the family; a R-rated popular culture; working mothers, latchkey childhood; MTV generation; greater willingness to take risks; greatest entrepreneurial generation; tech-savvy.

## **Millennials (1981 – 2000)**

This generation is known as Generation Y, Gen Y, the Net Generation, the Entitled Generation, or most commonly as Millennials. The last generation of the twentieth century have shed the high-risk behavior that was seen in the previous generation and tend to be drawn to large corporations or government for employment (Howe & Strauss, 2007). Even as such, they do not expect to remain in the same job for any length of time; they are transient employees, having no loyalty to organizations and seeking to gain the most broad experience they can in the workplace. They want relationships with their bosses and they appreciate immediate feedback and recognition (Verschoor, 2013).

The most significant aspect of this generation is their ability to assimilate information technology, as they are exceptionally technologically literate. They adapt well to information technology and instant-communication technologies as these have been integral parts of their lives since birth (Simons, 2010). Their ability to seamlessly embrace information technology in the workplace and their ability to multitask are what set them apart from the other generations (Wilson, 2009).

This generation grew up in the shadow of September 11, 2001 and, for this cohort, this is the most significant and defining moment to date. The recession that started shortly afterward created a negative environment for the Millennials and they are having problems finding employment. This is primarily due to the previously mentioned Boomers, who are not retiring due to the economic downturn so that they can build up their retirement savings. The Millennials are similar to Gen X in that they feel entitled. They have unrealistic expectations regarding the rate at which they feel they should progress at work. They are unlike previous

generations that felt the need to take their time and pay their dues to the organization before seeing a raise or promotion.

Table 4: Characteristics of Millennials

Author(s)	Characteristics of Millennials (Summary)
Simons (2010)	Known as Generation Y or Millennials; born 1977-1998; Born during the rise in globalization and instant communication technologies; came into a child-centric time where they were given much attention; characterized by self-confidence, team orientation, socializing in groups; prefer group work over individual work; They respect structure and hierarchy in the workplace; they enjoy having a relationship with their boss; great need for mentoring on the job.
Cekada (2012)	Known as Generation Y, Millennials, the Net Generation, the Entitled Generation; born 1981-2000; the most diverse generation in history; the most educated and the most technologically literate and advanced; given attention, they possess self-confidence that can be mistaken for arrogance.
Verschoor (2013)	Known as Millennials; lack fundamental literacy; short attention span; not loyal to organizations; demand immediate feedback and recognition; easily adapt to and integrate information technology in the workplace; do not seek a career in a single organization; they dress however they feel comfortable.
McCrindle and Wolfinger (2010)	Known as Generation Y; born 1980-1994; As young adults they live in the crisis period of post-September 11; They like to experiment and their peer groups are important in their lives; They tend not to possess brand loyalty, are credit dependent, and live a life of debt.
Wilson (2009)	Known as Millennials; born 1981-1999; marked by being technological savvy and by their innate ability to multitask; embrace diversity and multiculturalism; family-centric orientation viewed by earlier generations as needy, indulged, entitled, and self-absorbed.
Al-Asfour and Lettau (2014)	Known as Generation Y; born 1981-2000; Considered optimistic; embrace civic duty; display confidence and strive to become achievers.
Howe and Strauss (2007)	Known as the Millennial Generation; born 1982-2005; benefited from a child-centric culture where children were afforded many opportunities; declining high-risk behavior; drawn to large corporations or governmental jobs; they seek out teamwork and are risk-averse; desire a work-life balance.

## **Motivational Factors and Values**

In their book “Millennials Rising: The Next Great Generation,” Howe and Strauss (2000) stated that, aside from birth dates, there exist three characteristics that differentiate or define generations. The authors believed that birth year is actually a minor factor in differentiating the generations and they postulated that perceived membership, common beliefs and behaviors including their views of information technology and its role in their lives, and common location in history all play a larger role in defining the generation a person is from.

The first attribute, perceived membership, can be described as the self-appointed relationship that members of a generation identify themselves with. This self-identification will tend to begin in their teen years and to end when they enter adulthood or shortly afterwards. Perceived membership strays from the traditional birth date methodology that demographers predominantly use to identify generations. The use of perceived membership to determine a generational cohort can be affected by factors that are in fact not generational but sociological. An example of this is that Gen Xers in North America saw personal computers such as the Apple II, Commodore 64, and IBM XT as well as video games played on an Atari console arrive on the market, and they therefore self-identify with that generation. By all accounts, the introduction of home electronics such as these is one of the main attributes of Gen X. People from third world countries born in what is deemed the traditional Gen X birth years likely did not see the proliferation of such home electronics until a decade later due to availability and cost. Therefore, the perceived membership methodology is not as reliable as birth year when considering the global community.

The second attribute mentioned by Howe and Strauss (2000) is comprised of common beliefs and behaviors. These are the attitudes or beliefs that people possess with respect to their

personal and professional lives, their political beliefs, and their behaviors regarding events occurring around them such as crime and drug use, and regarding family issues such as marriage, children, and health.

The third attribute Howe and Strauss (2000) proposed is common location in history. Gelston (2008) stated that a generation is shaped by this attribute and that the formative years start at childhood. This attribute is defined by the events of the day, the significant political, economic, or historical events that mark or define a point in history. Examples of this for the various generations are:

- The Silent Generation: Japanese attack at Pearl Harbor on 07 December 1941 and WWII (1939-1945);
- Boomers: Vietnam War (1965-1973) and the landing on the moon (1969);
- Gen X: Space Shuttle Challenger explodes (1986), Fall of the Berlin Wall (1989); and
- Millennials: Columbine shooting (1999), Y2K (2000), 9/11 (2001).

Besides these three attributes proposed by Howe and Strauss (2000) and the traditional birth-year definition of a generation, McCrindle and Wolfinger (2010) propose that the traditional biologically-based generational definition is no longer applicable. They state that the traditional biological definition of a generation as being a 20 – 25 year span is now irrelevant as the generational cohorts are changing faster than those of previous generations and are now primarily influenced by ever-accelerating technological advances, the ability to change career and study options, and significant changes in societal values (McCrindle & Wolfinger, 2010). As such, the authors claimed that two decades is far too expansive when considering a generation. The authors went on to state that the biologically driven definition of generation is

further flawed as women are, on average, having children later in life by approximately six years, and this compounds the problem of defining generations according to a specific time span.

The three principle generations occupying the workforce and school today are the Boomers, Gen X, and Millennials. As such, for the remainder of this study, only these three generations will be compared and evaluated. The Silent Generation has been discussed only because it was highly influential on the Boomer generation and a small number from this cohort remained in the workforce into the 21<sup>st</sup> century.

### **Ethical Beliefs and Work Habits**

There exist significant differences between the three generations occupying the workforce today. These differences are cause for concern for executives and managers alike. Leaders of this multigenerational workforce are being tested in their leadership skills as each different generation has distinct ethical beliefs and work habits (Al-Asfour & Lettau, 2014). These generational differences can be referred to as a “generational gap,” a term that according to Simons (2010) was coined in the 1960s to describe the differences found between the Silent Generation and the Baby Boomer generation. This generation gap exists today and can be found in the workplace; the challenge is to determine how to bridge the gap.

Smola and Sutton (2002) examined generational differences in the values that the generations exhibit. The authors explained that, as the Millennial population continues to enter the workforce, they will soon be the largest generational cohort in the workplace. The challenges of a multigenerational workforce are significant and managers will need to understand the various unique characteristics and motivators in each generation in order to bridge the generational gap. If managers are not able to bridge the gap, they stand to experience significant challenges at work such as misunderstandings and miscommunication. If a manager is able to

bridge the gap and communicate effectively to each generational cohort, the manager will successfully create an environment where innovation and productivity thrive (Smola & Sutton, 2002). The authors concluded that work values change with the times, and their research concluded that there exist significant differences in values among the generational cohorts.

Gelston (2008) explored the problems arising in the workplace regarding generational differences and called this generation wars. Each generation possesses negative perceptions of the other generations. According to Gelston (2008), Gen Xers and Millennials see each other negatively in that Gen Xers see Millennials as a group of arrogant and entitled people while Millennials see Gen Xers as a group of whiners. Both Millennials and Gen Xers view Boomers as an annoying group of self-absorbed people who are nothing but workaholics. The author claims that 68 percent of Boomers feel that generations younger than theirs do not possess the proper work ethic and that this is a cause of problems in the workplace. Millennials acknowledge that there exist differences in work ethics between generations and 13 percent of Millennials think this difference is the cause of friction (Gelston, 2008).

Other authors describe the differences found in the workplace as toxic. Simons (2010) explained that it is important to understand the unique generational differences that exist in the workplace today to be able to effectively mitigate these issues. He explained this by outlining the three generations and comparing their defining attributes or characteristics. Verschoor (2013) outlined multigenerational workplace differences by explaining the differences in ethical behavior between the generations. Davis et al. (2006) explained specifically how Boomers and Gen Xers differ in work ethics, particularly in the IT profession. Wilson (2009) attributed the misunderstandings and tension in the multigenerational workplace to a difference in values.



Both Ludwick (2007) and Thielfoldt (2014) focused their attention exclusively on the Boomers and their contribution to the rifts in the workplace.

### **Boomers: Habits and beliefs.**

The primary characteristics of Boomers according to Simons (2010) are social change and affluence. Simons attributed this to the fact that Boomers grew up in the shadow of WWII in a time of prosperity and during a period of increased civil rights awareness. This generation is considered the wealthiest mainly due to the contributions of their parents, who had to endure the end of the Great War, the Great Depression, and WWII. This made their parents' generation highly cautious with finances, as they were determined to ensure they were not caught in the same predicament that they experienced during the Depression. The result of this caution, and the winning of the war, translated into a time of great affluence for Boomers. Boomers considered themselves to be a special generation and felt they were better than the generations before them. Their values and beliefs were shattered with the assassinations of Dr. Martin Luther King and President Kennedy.

According to Verschoor (2013), Boomers exhibit individualistic tendencies. They are considered self-centered yet self-motivated. This self-motivation drives them to become the best they can at work and they tend to become workaholics who have no time for feedback from others. Their general tendency is to be very optimistic and intensely competitive. They tend to prefer a casual and friendly workplace where they have the flexibility to be actively involved at work.

Boomers are also described as a generational cohort that is willing to make sacrifices for their careers. They are seen as the cohort that believes that an employee must "pay their dues" to the organization before reaping any rewards (Davis et al., 2006). These tendencies and values

are what set Boomers aside from later generations and are likely the driving force behind the workaholic tendencies Boomers are well known for.

Wilson (2009) examined the issues surrounding different generational cohorts in the workplace. This study found ways to create a harmonious multigenerational workplace in which the differences among the generational cohorts can be overcome. Wilson (2009) described various characteristics that can serve as guidelines to be aware of when managing Boomers in the workplace. The characteristics exhibited by Boomers include their desire or need for public recognition and for opportunities to leave a lasting legacy in their organizations. Their well-known workaholic tendencies provide them with the drive they need to maintain their competitive nature and make them strive for continual personal and professional development.

Ludwick (2007) and Thielfoldt (2014) exclusively examined Boomers in the workplace. Ludwick wrote in 2007, just before the economic downturn that affected much of the world. This is clear, as Ludwick made a number of assertions that have not come to fruition. The very title of his article, “The Boomers Are Already Gone,” reflects a common belief in the early years of the new millennium. Boomers had been saving all their lives, the economy was doing well, and it was the general expectation that Boomers would start retiring en masse starting around 2008 or 2009. Ludwick (2007) outlined how many organizations had started developing their succession plans, the subject was a popular topic at conferences, and governmental auditors were sounding the warning that a significant amount of corporate knowledge was about to be lost. One statistic that was offered was that it was expected that, by 2009, approximately fifty percent of the civilian workforce in the federal government and over 75% of those in the Department of Defence would be eligible to enter retirement. The Department of Labor estimated that there would not only be a mass exodus from the workplace, but that there would be a shortage of at

least 2.3 million workers by 2014. This exodus was long awaited by Gen Xers as they believed that the Boomers had been occupying leadership positions for too long already (Ludwick, 2007).

Thielfoldt (2014) wrote her article the same year that Ludwick had predicted the 2.3 million worker shortage that never happened. Because the Boomers needed to stay in the workforce longer to mitigate the negative effect of the economic downturn on their retirement savings, they found themselves still at work, much to the displeasure of the younger Gen X and Millennial generations. Thielfoldt looked at how managers can “rewire” their Boomer employees. Since the Boomers were not able to retire, and have spent at least seven years at work past the date they had originally meant to start their retirements, managers are struggling with Boomers, who had traditionally been workaholics, to help them to become motivated in the workplace. The US Census of 2010 indicates that Boomers accounted for 38% of the total workforce. According to Thielfoldt (2014), managers mistakenly believe they need to provide guidance and mentorship to the Millennials entering the workforce, even as Boomers have become the least engaged workers in the workplace and the most actively disengaged employees. As Boomers continue to occupy the workplace, it will be important for managers to reinvigorate this generation to bring them back to their once-reputed workaholic selves. It is highly likely that their lethargy is due to the length of time they have been in the workforce at this point. Thielfoldt made suggestions about what motivates and demotivates for Boomers and made recommendations to see Boomers return to being active members of the workplace once again.

### **Generation X: Habits and beliefs.**

Gen X are the middle children of the three generations being examined, and they display the classic middle child tendencies. The Pew Research Center has aptly described those belonging to Gen X as “America’s middle child” since this generation fall directly between the

ages of 34 to 49; they are in midlife, bookended by two larger generations on either side, the Boomers ahead and the Millennials behind. This generation, according to Simons (2010), has the distinction of being the generation that saw the rapid expansion of television and the beginning of high-tech products in the home such as personal computers and video games, to name a couple. This generation grew up in a world that was very different from that of their Boomer predecessors. This generation was also called the “latch key” generation, as many were parented either by single parents or by parents who were both employed. As children, Gen Xers would arrive home after school to find an empty home where they would need to fend for themselves until their parent(s) came home from work. This instilled in this generation a strong sense of self-sufficiency at a very early age. Simons explains how this has become one of the characteristics of this generation at work: Gen Xers do not like having someone looking over their shoulders; they prefer autonomy. With that in mind, Gen Xers prefer to have, or at least appreciate having, immediate feedback and are at ease providing feedback to others. Gen Xers are also known to work well within multicultural settings and they want their workplaces to be fun places to work (Simons, 2010). This generation was the first generation to see mass layoffs that affected their families, resulting in job insecurity due to the recession in the early 1980s. This has made them indifferent to organizations, as they do not possess the same loyalty to their employers that prior generations had. Gen Xers are comfortable stopping and starting their careers and making lateral moves as they do not possess the desire or drive to climb the corporate ladder. They value their bosses and their team members more than the organizations themselves.

Gen X has been labeled with negative stereotypes such as lazy, skeptical, and cynical. Given their independent nature, they tend to question authority, unlike previous generations.

They appreciate a work-life balance and appreciate the ability to maintain a flexible schedule.

These ethical generalizations presented by Verschoor (2013) are not substantiated; they are simply stereotypes that tend to follow Gen Xers. Verschoor outlined ways to incorporate ethics and compliance programs that would mitigate these stereotypical characteristics.

Davis et al. (2006) examined the work commitments of Gen Xers within the IT profession. They found that Gen Xers were classified as being lazier and as placing a low value on work and an unwillingness to make sacrifices for their careers at the expense of their personal lives; this is opposite to the Boomer mentality. These attributes are because Gen Xers grew up in a time of uncertainty; hence, they were required to fend for themselves. They saw their parents become victims of downsizing and restructuring resulting in job loss and hard financial times, leading Gen Xers to believe that there was no such thing as a secure job. This instilled in them a desire to become multitasking generalists who could transfer skills to other jobs, thereby increasing their marketability. While the authors acknowledged that there are noteworthy differences between Gen Xers and Boomers, they concluded that there are actually more similarities than differences between these two generations.

### **Millennials: Habits and beliefs.**

There is substantial literature regarding Millennials and their habits and beliefs, which are vastly different than those of previous generations. The Millennial generation has experienced the most noteworthy changes in their lifetimes, something that is likely asserted as each new generation comes into focus. Millennials have not known a world without the Internet, email, gaming consoles, MP3 players, personal computers, and tablets, and these have influenced Millennials' habits and beliefs in a meaningful manner.

The rapid proliferation of communication technologies is the chief characteristic of the Millennial generation according to Simons (2010). This has led them to become proficient at multitasking and has allowed them to develop as effective team players that prefer teamwork to individual endeavors. This generation is new to the workplace and therefore is in need of mentoring. As they respond well to teamwork, mentoring is something Millennials seek out; they desire one-on-one instruction and direction and respond well to it. They appreciate stability in the workplace and value leadership and guidance.

They grew up at a time when the self-esteem movement was at the forefront and all children were declared winners; there were no losers. This instilled in this generation a sense of entitlement, one that needs close mentoring and supervision. When Millennials find themselves in an ambiguous situation without clear guidance or direction, they begin to struggle (Gilburg, 2008). They are unable to take action on their own as they expect an authoritative figure to give them direction.

Verschoor (2013) outlined various negative traits Millennials possess. For instance, he stated that they are known to have short attention spans and do not exhibit loyalty to organizations as they realize they will experience a variety of different jobs. On the other hand, this generation is able to seamlessly integrate information technology in the workplace, something prior generations are not as adept at doing. An ethical challenge facing Millennials according to Verschoor (2013) is that they feel pressure to break ethical rules in the workplace. They do this because they are more susceptible to feeling pressured by others in the workplace. Verschoor's study also indicated that this generation sees more ethical misconduct at work than the other generations and are less likely to report the misconduct. According to Verschoor, Millennials observed almost half of the workplace misconduct that took place, including things

such as personal business on company time, lying, abusive behavior, computer resource abuse, and discrimination (Verschoor, 2013). Of the Millennials who observed misconduct, 67% reported it; the types of infractions reported were theft, falsifying financial claims, bribery, and falsifying hours worked. Verschoor detailed the various infractions and ethical problems that can be found in the workplace. Most importantly, the findings indicate that younger workers tend to ignore misconduct at work if they feel it will prevent job loss. They accept the use of bad or immoral methods to accomplish positive results, an attitude other generations do not support (Verschoor, 2013). This belief, which may be framed as a lack of ethics, will certainly influence cyber security, as Millennials may feel justified in ignoring security policies.

### **Generational Perspective on IT Purpose and Functionality**

Each generation views IT and IS through a different lens. Extensive literature exists regarding the digital fluency of Millennials but that of other generations is merely superficially examined. This is mainly due to the fact that Millennials, or the Net Generation as they are sometimes called, have grown up enveloped in a digital world. Multigenerational workplace tensions can be partly attributed to the perspective each generation has on how work is accomplished and on the role of information technology within the workplace (Simons, 2010). The generational gap that exists with respect to the integration of information technology in the workplace is classified as the most noticeable gap according to Simons (2010). Gelston (2008) explained that there is significant tension in multigenerational workplaces due to the use of information technology and due to differing work ethics.

Notable Boomers Bill Gates and Steve Jobs brought digital technologies to the forefront, making such technologies affordable to the masses; this in turn made it possible for households around the world to integrate digital technologies into their daily lives. The Boomer generation

in general was on the late end of the information technology spectrum, as they did not grow up with digital technologies in the home. Their innovative technologies were items such as the 8-track tape player, color television, and the audiocassette. While they have done a good job of familiarizing themselves with this new digital paradigm, they generally make use of it only superficially and are challenged by its integration into the workplace. They view information technology at the workplace differently than their younger peers, as they do not view IT solutions holistically but instead see IT applications as discrete solutions to address specific or individual needs (Simons, 2010). It was at the workplace that Boomers were first introduced to and learned about information technology, and they use it as they feel it improves personal productivity (Houck, 2011).

Gen Xers were the first generation to experience the influx of information technology at school and home. This eventually spread to the workplace, where Gen Xers had already been for some time when information technology in the workplace became mainstream. Gen Xers are a technically smart generation and they see the benefits of information technology in the workplace. This generation has become well integrated with information technology both at home and work. Gen Xers learned their technological skills at school as personal computers became popular, and they feel information technology is critical for both their personal and professional lives (Houck, 2011).

Beyers (2009) referred to the Millennial generation as the Net Generation. He depicted them as a smart and impatient generation, one that has been continually exposed to visual messages and multimedia since birth. This depiction was corroborated by Gilburg (2008), as she stated that the Millennial generation has been called the most technologically sophisticated and high-performing generation and also the most high-maintenance. Houck (2011) stated that this



generation believes that information technology is at the very core of life and work. Their ability to handle information technology greatly exceeds that of the previous two generations, and they feel information technology is an essential component of how they live, work, and think (Kilber, Barclay, & Ohmer, 2014; Simoneaux & Stroud, 2010).

Millennials belong to the global community, a community that can be readily found online (Beyers, 2009). They possess a large array of electronic devices that allow them to remain in continuous contact with their friends, colleagues, and coworkers. This has enabled them at the workplace by increasing their ability to multitask. Millennials are a smart generation, a generation that expects and demands immediate results from themselves and others. They are able to accomplish this as they have access to large amounts of data, and they use the digital tools at their disposal to rapidly sort through the volumes of raw data in their electronic files to find what they are looking for.

This preference for electronic documents among Millennials enables them to make extensive use of Information Commons such as libraries and online communities, according to Lippincott (2010). Given Millennials' propensity for teamwork and work in team settings, Information Commons are merely an extension of this preferred meeting place. Millennials interact extensively with their electronic devices and use digital forums with the same ease as previous generations gathered and communicated in coffee shops (Lippincott, 2010).

The ease with which this generation is able to multitask and interact instantaneously via digital means on a 24-hour basis ensures that Millennials, by default, remain the dominant digital generation in the workplace. This tendency to multitask has led Prensky (2001) to state that the brains of the millennial generation function differently than those of the generations that preceded them. As previously described, the average Millennial grew up surrounded by

electronics at their disposal, and Prensky asserted that the intensity of activity Millennials have experienced since childhood in both video games and other digital media has affected how their brains work (Prensky, 2001). This is a conclusion that other authors have also arrived at, and it is one of the defining characteristics of Millennials (Beyers, 2009; Lippincott, 2010; Prensky, 2001).

The greatest strength Millennials possess in the workplace is digital fluency and a technological sophistication that demands their engagement in the information systems that run organizations. This fluency enables Millennials who want to integrate mobile and consumer technologies into the workplace. IT departments already find it challenging to maintain positive control over management and security risks that these mobile technologies pose to their networks (Gilburg, 2008). As more Millennials enter the workforce and expect or demand heavier integration of their mobile devices, IT departments will need to accommodate these new technologies, as this is the way Millennials work best.

The Gen X and Boomer generations have embraced information technology in the workplace, yet there is a notable distinction that separates them from millennials: paper. Boomers and Gen Xers are both able to work in a high-tech environment, yet when reading books or lengthy documents, these two generations prefer to hold paper in their hands whereas Millennials do not have a problem using a laptop or tablet to do the same (Simons, 2010). Boomers and Gen Xers continue to fill metal filing cabinets and paper folders with paper records, while Millennials fill their electronic filing cabinets and folders with electronic documents.

Communication methodologies are another generational gap inspired by the use or non-use of information technology. Both Boomers and Gen Xers prefer face-to-face conversations or

telephone calls to conduct their business communications, whereas Millennials prefer to use either email or text messages. The two older generations are of the opinion that electronic communication is abrupt and can be easily misunderstood by the Boomer or Gen X reader. The older two generations feel that electronic communications are not the way to build business relationships (Gelston, 2008). As technology continues to evolve, it will become more difficult to bridge the technological gap between Millennials and the two older generations as the gap will continually broaden (Simoneaux & Stroud, 2010).

The three generations are all engaged with information technology in the workplace and recognize the efficiencies it brings through its integration in day-to-day work. Many organizations use dated applications, yet these applications are their lifeblood. Millennials, who prefer a fast-paced, multitasking environment, see these dated applications as obstacles that prevent efficiency at work. Millennials are looking for enterprise solutions that are systemic, electronic, and portable, and which therefore pose significant challenges to IT departments (Simons, 2010).

### **Preferred Training Methods**

Traditionally, training methodologies varied depending on the type of course, program, or institution. Educators have examined the influence generations have on education and how these differences should be considered in instructional design, and researchers have studied the training methodologies best suited to particular generations (Cekada, 2012; Farrell & Hurt, 2014; Reeves & Oh, 2008). In a study conducted for IBM, Lesser and Rivera (2006) discovered that differences are real and that there exists a need to diversify the methodology and content of the training being offered to appeal and be beneficial throughout the multigenerational workplace.

Each generational cohort responds differently to different learning styles, and by understanding which methods work best for the different generations, instructional designers will be better prepared to design effective training plans (Cekada, 2012; Farrell & Hurt, 2014). This will ensure that organizations are better able to train and prepare their multigenerational workforce. Organizations are beginning to realize that, given the ongoing and future retirement of the Boomer Generation, there will need to be a transfer of knowledge from the Boomers to the Millennials, and that well-thought-out training will facilitate this knowledge transfer (Farrell & Hurt, 2014).

As previously discussed, Boomers did not have digital technologies in their childhoods. It was not until they were well established in their careers that they first saw computers and other IT and IS enter their workplaces. This is where Boomers first learned about IT, and they applied it as best they could to what their functions were at their jobs. The Boomers' learning style was the traditional teacher-led style with chalkboards, and with paper notebooks for note-taking and homework; no information technology existed in the classroom. This generation did not experience or expect any type of entertainment in the class. There was no need to become overly engaged in class, as the traditional lecture format they were accustomed to did not include this (Bell, 2008; Cekada, 2012).

Boomers were experiential learners; they preferred to learn through methods such as case studies. They preferred to learn in small class settings where they could share their experiences and debate issues. Boomers want to be able to see the value in what they are learning and want to be able to apply their new knowledge at work or home. Since they did not experience information technology until later in life, they are hesitant about, and typically resistant to, strong technological change unless they can be shown how this change will result in a demonstrated

value for them personally or at work. Boomers tend to possess individualistic tendencies and, since they were educated using traditional methodologies, they prefer to work alone and not in groups or teams (Cekada, 2012; Howe & Strauss, 1991).

Generation X is a generation that values education and training, particularly in the workplace, and they view it as a way to get ahead and succeed at work. One-on-one mentoring, coaching, and on-the-job training are types of training methodologies to which Gen Xers respond well (Houck, 2011). Gen Xers are active learners who, when engaged, can learn quickly and are able to accomplish learning through on-line and similar types of self-directed courses. (Farrell & Hurt, 2014).

Gen Xers were still in school when digital technologies and personal computers became common in homes and schools. Early Gen Xers were entering high school when the first Apple II and IBM XT PC computers were being distributed and computer classes became available for them in school. This allowed them to be at ease with any type of learning methodology; they can easily adapt to flexible learning methods, whether it be the traditional method, self-study using traditional correspondence courses, or high-tech multi-media courseware. Gen Xers have a more comfortable attitude toward, and a greater ability to learn using, information technology than their predecessors' generation.

This generation does not enjoy reading as much as the other two generations; therefore, learning materials should not include lengthy, superfluous documents. Booklets such as Cliffs or Coles Notes that consolidate information and allow the Gen X reader to quickly grasp pertinent information up front will result in better learning for Gen Xers (Bell, 2008; Cekada, 2012).

The characteristics of this generation include a strong desire for independence, a preference to be involved at work, and a desire to work in relaxed settings. These characteristics

parallel their preferred learning environments, which are casual, relaxed environments where they can have fun learning (Cekada, 2012). Gen Xers also enjoy being challenged and want to be able to incorporate their learning into the overall organizational strategy (Bell, 2008; Cekada, 2012; Reeves & Oh, 2008).

Information technology has influenced Millennials since birth, and has played a significant role in their learning and in their preferred learning methodologies. This generation has been exposed to constant stimulation from technology, and this has affected the way they adapt to learning. Prensky (2001) called them digital natives and claimed that this constant exposure to information technology since birth has changed the way their brains work. He also stated that, since Millennials have grown up with constant stimulation, they don't simply think about things differently: digital natives think differently as a result of the digital environment they grew up in (Prensky, 2001). They are therefore very comfortable with information technology and prefer to use it in learning environments.

Millennials are commonly characterized as being efficient at multitasking, and this has given them short attention spans. They do not enjoy long, drawn-out lectures and much prefer short bursts of learning with breaks every 15 to 20 minutes. During their breaks, they enjoy being entertained with jokes or simply using their electronic devices to check any one of their commonly used applications for updates. These learners are visual learners and they prefer multimedia to traditional reading of textbooks. Their short attention spans mean that they want to receive answers quickly. They enjoy learning in collaborative or group settings, working in teams, and getting immediate feedback (Cekada, 2012).

## **Cyber Security Awareness and Governance**

Cyber security awareness is becoming a growing issue within organizations as the use of IT and IS becomes critical for business operations. To ensure that organizations remain viable and effective, they need to protect their information holdings, and to do this they must employ effective cyber security awareness. The literature describes cyber security awareness in terms of internal programs and education that make employees at all levels aware of policies and effective practices (Mohamad Rashid, Zakaria, & Nabil Zulhemay, 2013; D. W. Straub & Welke, 1998). Most research studies, textbooks, and industry publications indicate that the single weakest link in cyber security is people. For the purpose of this study, only NMSVs will be examined. Malicious attacks that involve insider hacking, theft, or purposeful criminal activity will not be explored. The research will be limited to inadvertent, accidental, or negligent cyber security violations.

One of the most significant issues facing organizations is the poor cyber security posture of its employees. A lack of knowledge on the part of employees in an organization makes information systems vulnerable within the organization. Education and training are cited as being key components in raising the awareness of employees. Security policies are what protect the digital assets of the organization, and these policies are only effective if employees are both aware of and comply with the policies (Dutta & McCrohan, 2002; Mohamad Rashid et al., 2013). It is not enough to just write policies or governance documents; the target audience for these policies must be aware that the policy exists and they need to be educated in the reasons for the policy and how it protects the organization and the employees' employment. While companies have attempted to mitigate security infractions with training, the results are not always as expected. Despite employees receiving a minimal amount of training, they were found

to have continued with insecure practices such as writing down passwords or creating simple passwords that are easy to guess (Wylder, 2003).

Employees put their organizations in significant harm's way when they do not adhere to organizational cyber security. Siponen, Mahmood, and Pahlila (2009) examined the risks employees posed when they ignored organizational security policies. When employees are unaware that what they are doing exposes the organization to unnecessary risk, they become complacent and do not feel the need to follow organizational policies regarding security. It is therefore important to ensure that employees are made aware of and realize the risk they are subjecting their organization to through their non-compliant habits. This would then ensure that employees have a strong intent to comply with the policy, as they would see how their actions could be detrimental. Effective and visible security awareness campaigns and educational programs are able to mitigate such undesired behavior (Siponen et al., 2009).

Many organizations spend a considerable amount of time and a significant portion of their budgets on security awareness campaigns in attempts to make their systems more secure. Technical solutions are implemented in server rooms, solutions that include encryption, firewalls, antivirus protection, and intrusion protection. Executives are surprised when these technological security solutions fail because the executives themselves failed to implement an effective awareness campaign. Security solutions lose their efficacy when users do not adhere to organizational security policies (Holbert, 2013; Puhakainen & Siponen, 2010). While it would seem obvious that organizations would feel the need to make security awareness programs a priority and to allocate the proper funding, a study by Keller, Powell, Horstmann, Predmore, and Crawford (2005) indicated that, statistically, this was not the case. The authors found that many small businesses placed employee training at the bottom of their priority lists for IT spending.



The primary factor an organization should consider in the enhancement of their security posture is effective governance. Through effective governance, industry best practices with respect to cyber security training and awareness, policy, and procedures development will be incorporated. It is not enough that policies be written; adherence to these policies is essential in order to meet the intent of the governance as it is set out (Wylder, 2003).

Governance ensures that the organization is able to incorporate a holistic cyber security enterprise solution. The executive level should direct governance; policies will then define the overarching regulations and expectations of all employees. The relationship between cyber security and corporate governance was examined by Von Solms (2001), who concluded that good corporate governance should include the role and importance of information security.

In 2014, Target retail group compromised the credit card information of 40 million clients and the personal information of 110 million customers through hacking. JP Morgan compromised the personal information of 80 million clients, and, at Sony and Apple, over 110 million customers were prevented from using the companies' gaming systems due to a cyber attack. It is becoming more common to see cybersecurity governance (CSG) enter the boardroom of major companies around the world. CSG is becoming widely accepted as an essential part of corporate governance, and boards realize that accountability for safeguarding electronic data falls to the board members, not to technical staff members. Companies are fully reliant on computer systems and are integrating all their business processes onto their networks (Von Solms, 2015). Von Solms (2015) made four recommendations for boards to get positive control of cyber security within their organizations:

- Cyber and information security expertise must reside on the board on a permanent basis,

- Cyber and information security must be a fixed item on the agenda,
- Reporting and measuring metrics must be incorporated for the board to maintain situational awareness of the security status of the organization, and
- Board members must understand their fiduciary obligation with respect to the protection of personal information.

Top-level managers play a significant role in shaping their employees' compliance behavior by influencing the corporate culture regarding security behaviors since cyber security is not only a technical IT issue but a leadership and management issue (Dutta & McCrohan, 2002). Mainstream media tends to headline only hacking carried out by criminals and computer hackers; however, research has shown that organizations are at far greater risk from their own employees' actions. These types of actions demand that organizations implement comprehensive governance that incorporates comprehensive security awareness education and training plans. These plans should outline the essential education staff must undertake to become better educated. The literature has outlined the need for different education or training requirements to exist at the different levels of employees. End users will need different training than managers, IT staff, or executives. Research conducted by Mohamad Rashid et al. (2013) delineated the different users and the levels of training they require to possess a minimum level of knowledge (Hu et al., 2012; Mohamad Rashid et al., 2013).

Security policies are developed as a high-level plan that outlines the framework for ensuring corporate security of organizational data holdings. As has been mentioned, humans are the weakest link in the cyber security framework. NMSVs sometimes occur without users realizing they are doing something that will jeopardize the integrity of the organizations' security posture. Lim, Teo, and Loo (2002) explored what they called "cyberloafing." Cyberloafing is a

term coined to describe habits of employees with access to the Internet at work. In their study, the researchers found that email and recreational surfing of the web were the two main cyberloafing habits, with 84% and 90% of employees engaging in this type of behavior. While the Internet has enabled business to embrace rapid communication and access to data, it also poses a threat to organizations. When employees are not effectively trained in cyber security awareness, they will be more likely to commit NMSVs as they unwittingly expose their organizations to potential viruses and hackers.

Cyberloafing attitudes in employees change when they believe their online actions are being monitored (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009). Cyberloafing occurs when employees believe that their actions are not being monitored and they feel free to roam the World Wide Web at their leisure. There has been a noticeable increase in the proliferation of malicious code developed specifically to target organizations and their data holdings. Organizational security managers and cyber security managers put in place comprehensive technical solutions to maintain security, and the actions of employees render these technical solutions meaningless. Research revealed that when employees believe they are being monitored, they tend to comply with organizational security policies (Boss et al., 2009; Lim et al., 2002).

### **Cyber Security Awareness Training**

As end users pose the most significant threat to the cyber security posture of an organization, the intent in developing a security awareness program is to ensure that users understand organizational security policies and best practices and put them into practice. The propagation and popularity of wireless networks and access points, coupled with the default

corporate use of the Internet, has made it challenging for organizations to implement IS Security (Guo et al., 2011).

D. W. Straub and Welke (1998) researched the issue of systems risk, which they defined as “[t]he likelihood that the firm’s information systems are insufficiently protected against certain kinds of damage or loss.” The authors stated that it is possible for managers to mitigate, manage, or reduce risk if they are aware of the controls available to them and use the controls effectively. Managers who do not understand the full complement of controls available to them and do not implement them correctly will experience less effective security. To mitigate systems risk, the researchers proposed a security awareness program that includes both managers and end users, each requiring different education. Managers will become familiar with the security action cycle, a framework based on the deterrence, prevention, and detection framework (D. W. Straub & Welke, 1998; J. D. W. Straub & Nance, 1990; Straub Jr, 1990). All users throughout the organization, regardless of their positions, should engage in the security awareness training that covers organizational strategic objectives as well as lower-level vulnerabilities (D. W. Straub & Welke, 1998).

Recent increases in globalization in combination with technological advances have become a double-edged sword for companies as international criminal groups have become empowered. These organizations are now able to conduct sophisticated, increasingly frequent and severe attacks on computer security systems (McCrohan et al., 2010).

The goal of security awareness training is to change behaviors and minimize the potential for NMSVs and computer abuse by raising individuals’ security awareness. Only through an aggressive and strong security awareness program will organizations be assured of the security, confidentiality, availability, and integrity of their data (Mohamad Rashid et al., 2013; Siponen &

Vance, 2010). The human component plays a large role in cyber security and, as such, it must be the focal point of any security awareness program (Holbert, 2013). Scholars and researchers have long recognized the importance of cyber security, and their findings reflect important differences regarding the causes of noncompliant behavior (Hu et al., 2012).

Puhakainen and Siponen (2010) examined the issue of IS security training and employee compliance using action research. The researchers reviewed and tabulated twenty-three studies regarding IS security training and outlined the authors and key findings. A review of the key findings results in the realization that there are a number of different proposals regarding the best way to conduct IS security training. Various key findings proposed identification of the target audience for the training; however, the variable used in the identification of the target audience was their function or position in the organization. None of the key findings include an examination of, or recommend the use of, generational considerations as a factor or variable in the development of IS security training.

### **Factors Influencing the Perceived Security Awareness Level of End Users**

Decker (2008) developed the Decker survey tool, which looked at four distinct factors and their influence on the perceived level of security awareness of end users. The factors included internal, external, and inherent factors. The internal factors are further divided into internal IT factors and internal management factors.

#### **Internal IT Factors**

Decker's (2008) internal IT factors examine the primary methods organizations use to influence security awareness. These methods traditionally include a holistic approach to network and information security. The methods that are most commonly used include organizational

security awareness training, acceptable use policies, and policies and procedures that are expected within the organizations.

Cyber security awareness is described in literature in terms of internal programs and education that make employees at all levels aware of policies and effective practices (Mohamad Rashid et al., 2013; D. W. Straub & Welke, 1998). An effective security awareness campaign can only be achieved through an effective organizational security policy (Holbert, 2013).

Appropriate password protection and frequency of password changes, initial security awareness training and education, and acceptable use adherence are all influenced by organizational policy. End users who are better informed and aware of these policies are less likely to adopt behaviors that cause NMSVs (Guo et al., 2011). The most significant threat to the cyber security posture of an organization is a disregard for or lack of compliance with organizational cyber security policy (Holbert, 2013; Siponen & Vance, 2010).

### **Internal Management Factors**

Internal management factors examine the behaviors and attitudes displayed overtly by the management staff of an organization. End users' perceptions of the management's commitment to organizational cyber security will affect end users' personal attitudes toward the organizational policy (Holbert, 2013). The organization's management is responsible for providing the resources required to ensure that policy is effectively delivered and that employees have the opportunity to engage in security awareness training and continually refresh their knowledge or upgrade it as required.

When management is seen by employees as taking a proactive approach to security awareness and leading by example, end users or employees react positively (Holbert, 2013).

Management must be seen as being serious about security awareness and adherence to policies,

openly discussing security awareness with employees on a regular basis, and ensuring that employees are not only aware of the penalties for breaches but become aware of the policies by attending training (Decker, 2008).

### **External Factors**

Of these four factors, external factors are the ones least researched in regard to their influence on security awareness (Decker, 2008). A number of external factors should be taken into consideration when examining the perceived level of security awareness of end users. The primary external factor influencing the security awareness level of end users is the media. End users receive reports and media stories regarding security breaches in high-profile cases, and this has a direct influence on end users' perceptions of their own organizations. Users are also influenced by external factors when they receive notices from institutions such as their bank warning them that they should be cautious when using Internet banking and how to avoid becoming a victim of fraudulent email or phishing.

Other external factors that may influence the behavior of end users are federal or state regulations, their own levels of use of anti-virus software, and the levels of information security training they have received outside of the workplace (Holbert, 2013). These external factors all play a role in end users' perceptions of and adherence to information security.

### **Inherent Factors**

Individualistic characteristics play a role in end users' levels of security awareness. What motivates end users will factor into and affect their adherence to organizational cyber security policies. End users' motivation to comply with organizational policy, attend training, and increase their technological knowledge contributes to the inherent factors. The culture of the organization should also be considered among the inherent factors. Some organizations require

their end users to exercise extreme caution in the IS/IT or cyber environment. An example of this would be employees in any national intelligence agency where breaches of security negatively affect the security of a nation. These employees will possess an organizational culture that employees at a retail store need not possess.



### **CHAPTER 3. METHODOLOGY**

This study used non-experimental quantitative methods to investigate the influence a multigenerational workforce has on the security awareness of end users by using Decker's (2008) security behavior factors. This study examined the effects of the multigenerational workforce on NMSVs by end users, which account for over fifty percent of security breaches (Holbert, 2013; Siponen & Vance, 2010). Decker (2008) studied end users' security behavior based on internal IT, internal management, external, and inherent factors. End users' security awareness was measured against these four factors to determine which factor had the most significant effect.

Cyber security policy violations negatively affect organizations, requiring them to adopt methodologies to educate the multigenerational workforce to create a corporate culture of cyber security. The intent of this study is to increase the body of knowledge regarding best practices and practical awareness training methodologies that can influence positive change in a multigenerational workforce. While there exists research that examines the factors affecting end user security awareness, no research can be found that examines and compares the cyber security awareness of different generational cohorts within the multigenerational workforce. By increasing compliance with organizational cyber security policies through effective security awareness training, corporate losses in terms of financial and intellectual property and data can be minimized.

#### **Research Design**

The study used a non-experimental quantitative research design and a survey instrument developed by Decker (2008) to explore generational differences in the factors affecting organizational cyber security policy awareness. The research examined the factors considered

by Decker (2008) that affect the security awareness of end users. These factors include security awareness training (internal IT factors), commitment on the part of management (internal management factors), and external and inherent factors. The factors were examined generationally to understand how each generational cohort viewed the importance of each factor and how this influenced organizations' cyber security postures. The survey instrument was designed to examine these four factors, and generational attributes defined how each generation viewed these factors.

### **Sample**

The sample for this study was a river sampling provided by Survey Monkey, an online survey company. Each generational cohort being examined received an identical survey. The generational cohorts receiving the survey were the Baby Boomer generation, Generation X, and the Millennial generation (Cekada, 2012; McCrindle & Wolfinger, 2010; Simons, 2010).

The sample needed to be broad enough to capture a suitable sample size for each generational cohort. In similar studies, Decker (2008) collected results on 99 respondents while Holbert (2013) collected results on 272 respondents. The suitable sample size for each cohort was achieved by conducting three surveys, one for each cohort, in an attempt to obtain an approximately equal sample size from each. The researcher's goal was to obtain results from 100 respondents from each cohort for a total of 300 survey respondents, in line with Holbert's (2013) sample size. This method was chosen over a single survey, as a single survey would provide an unpredictable sample size from each generational cohort. Within each generational cohort, a random sample was obtained, allowing an equal probability of being selected among all participants (Stokes, 2011). A generational cohort within a broad spectrum of positions from a range of organizations formed the randomly selected sample.

This study did not use secondary sources. The strategy was to use the survey instrument to gather the predetermined population size for each generational cohort. Through consultation with the researcher's mentor, the population size was determined.

### **Survey Instrument**

Decker's research instrument was used to measure the research study question (Decker, 2008). Permission was granted to use the survey instrument Dr. Decker developed. The survey began with a brief section of demographic questions, followed by twenty-five questions that were divided into five sections related to cyber security awareness (Appendix B). The five sections asked questions related to internal IT factors, internal management factors, external factors, inherent factors, and perceived security awareness level.

### **Hypotheses**

The study evaluated the relationships among the independent variables presented in the survey. Internal IT, internal management, external, and inherent factors were used to determine the influence of end users on the dependent variable, security awareness.

RQ1: What is the relationship between internal IT factors and the cyber security awareness of end users from each generational cohort?

H1<sub>01</sub> = Internal IT factors are not significantly related to the security awareness of end users of the Baby Boomer generation.

H1<sub>a1</sub> = Internal IT factors are significantly related to the security awareness of end users of the Baby Boomer generation.

H1<sub>02</sub> = Internal IT factors are not significantly related to the security awareness of end users of the Gen X generation.

H1<sub>a2</sub> = Internal IT factors are significantly related to the security awareness of end users of the Gen X generation.

H1<sub>03</sub> = Internal IT factors are not significantly related to the security awareness of end users of the Millennial generation.

H1<sub>a3</sub> = Internal IT factors are significantly related to the security awareness of end users of the Millennial generation.

RQ2: What is the relationship between internal management factors and the cyber security awareness of end users from each generational cohort?

H2<sub>01</sub> = Internal management factors are not significantly related to the security awareness of end users of the Baby Boomer generation.

H2<sub>a1</sub> = Internal management factors are significantly related to the security awareness of end users of the Baby Boomer generation.

H2<sub>02</sub> = Internal management factors are not significantly related to the security awareness of end users of the Gen X generation.

H2<sub>a2</sub> = Internal management factors are significantly related to the security awareness of end users of the Gen X generation.

H2<sub>03</sub> = Internal management factors are not significantly related to the security awareness of end users of the Millennial generation.

H2<sub>a3</sub> = Internal management factors are significantly related to the security awareness of end users of the Millennial generation.

RQ3: What is the relationship between external factors and the cyber security awareness of end users from each generational cohort?

H3<sub>0</sub>1 = External factors are not significantly related to the security awareness of end users of the Baby Boomer generation.

H3<sub>a</sub>1 = External factors are significantly related to the security awareness of end users of the Baby Boomer generation.

H3<sub>0</sub>2 = External factors are not significantly related to the security awareness of end users of the Gen X generation.

H3<sub>a</sub>2 = External factors are significantly related to the security awareness of end users of the Gen X generation.

H3<sub>0</sub>3 = External factors are not significantly related to the security awareness of end users of the Millennial generation.

H3<sub>a</sub>3 = External factors are significantly related to the security awareness of end users of the Millennial generation.

RQ4: What is the relationship between inherent factors and the cyber security awareness of end users from each generational cohort?

H4<sub>0</sub>1 = Inherent factors are not significantly related to the security awareness of end users of the Baby Boomer generation.

H4<sub>a</sub>1 = Inherent factors are significantly related to the security awareness of end users of the Baby Boomer generation.

H4<sub>0</sub>2 = Inherent factors are not significantly related to the security awareness of end users of the Gen X generation.

H4<sub>a</sub>2 = Inherent factors are significantly related to the security awareness of end users of the Gen X generation.

H4<sub>03</sub> = Inherent factors are not significantly related to the security awareness of end users of the Millennial generation.

H4<sub>a3</sub> = Inherent factors are significantly related to the security awareness of end users of the Millennial generation.

### **Data Collection**

Survey Monkey, a web-based survey portal, distributed the survey. Random candidates within a generational cohort received from Survey Monkey an email inviting them to participate in the survey and containing a link to the survey. The email invitation contained a letter of consent that outlined the purpose of the research and allowed potential participants the opportunity to decline the invitation. Participants indicated their willingness to partake in the study by selecting the link that took them to the survey. By selecting this link, the participants thereby agreed to accept all risks associated with the survey. Participation was completely voluntary, and no participant was compelled to provide information (Creswell, 2013).

Participants were able to stop taking the survey at any time. The survey was conducted over a one-week period in October 2015. The email inviting participants was sent out on 10 October 2015 to the Survey Monkey community. From that group, 342 completed the survey, 115 from the Baby Boomer Cohort, 113 from the Gen X cohort, and 114 from the Millennial cohort. A review of the participant surveys was conducted to ensure that the data were usable, and any surveys that were not completed were not used. The data collection included the export of the results from the Survey Monkey web portal to Microsoft Excel. The data were then imported into Statistical Package for Social Scientists (SPSS) version 22 for analysis. Survey data will be kept securely and will be destroyed after seven years.

## **Data Analysis**

Survey Monkey compiled the survey results, which were saved in a format compatible with Microsoft Excel and imported into SPSS for analysis. Inferential statistics were used to conduct the analysis of the data, thereby identifying both the subjects and the methods to be used (Creswell, 2013). Descriptive statistics were used to describe the basic features of the data obtained, providing tabular, graphical, and numerical summaries of data (Anderson, Sweeney, & Williams, 2014).

The Decker survey instrument consisted of a demographic section followed by five additional sections; of these, four sections separately addressed each of the four factors affecting security awareness among end users (internal IT, internal management, external, and inherent factors) and one focused on perceived levels of security awareness.

## **Validity and Reliability**

The Information Security Faculty at Capella University previously validated the Decker research instrument (Decker, 2008). Twelve professionals performed this validation by completing and analyzing the survey (Decker, 2008). These twelve professionals at Capella University assessed Dr. Decker's survey instrument for readability, clarity, and usefulness in gathering relevant data (Decker, 2008). Of the twelve, nine of the participants were in positions similar to the expected respondent population. Their positions ranged from front line staff to those in management positions. The remaining three participants were employed in the IT security field. Decker made minor changes to the survey tool after conducting the validation; these included modification of two questions and rewording of two others. Once Decker had completed the data collection, he calculated Cronbach's alpha in order to ensure consistency within the five sections of the survey.

### **Ethical Considerations**

Creswell (2013) explained that when research is performed using human subjects, the research plan must be reviewed by an Institutional Review Board (IRB). Researchers are required to submit their research plans to the IRB for approval prior to commencing their research to protect the participants from any human rights violations (Creswell, 2013). The researcher submitted the research plan to the Capella University IRB before commencing any research. As it is possible for ethical issues to come from the data collection during the research, the rights of participants are paramount and the participants' confidentiality and privacy were protected accordingly. Data were collected through the web portal in a manner that allowed the participants to remain anonymous. The data could not be attributed to or associated with the participants as no personal identifiable information (PII) was requested of participants in the survey.



## CHAPTER 4. RESULTS

This chapter discusses the outcomes of the research to better understand the generational differences in the factors affecting cyber security awareness. The research was performed using a quantitative method approach using the Decker (2008) survey instrument. A self-administered and closed-ended survey was used to gather information on the research questions, and the survey was distributed separately to members of the three different generational cohorts examined. The distribution of the survey to the different cohorts ensured equal representation from each generational cohort, specifically the Baby Boomer, Generation X, and Millennial cohorts.

The survey instrument began by collecting demographical information from the respondents, the results of which were explained then displayed using histograms. After completing the demographical information portion of the survey, respondents were given the opportunity to answer questions related to the independent variables affecting security awareness. The independent variables affecting perceived levels of security awareness were internal IT factors, internal management factors, external factors, and inherent factors. These factors determined the levels of security awareness of end users. The section focusing on each of these factors contained a group of questions that indicated the influence the particular factor had on the perceived level of security awareness of the respondent.

The results for each factor were separated into generational cohorts and analyzed for normality using both scatterplots and *QQ* plots. Upon confirmation of a positive linear relationship between the independent and dependent variables, the Pearson Correlation was conducted to examine the correlation between variables. Finally, an analysis of variance (*ANOVA*) was conducted to explore the significance of the variables. These results were

explained and displayed through tables and graphs. The evaluation and analysis of the data collected is the subject of Chapter 5.

### **Sample and Setting**

The 342 participants from the Survey Monkey community accessed the survey through the online portal in October 2015. The three generational cohorts examined, the Baby Boomer generation (1946-1964), Generation X (1965-1980), and the Millennial generation (1981-2000), received identical surveys to ensure equal representation. While the Millennial generation includes people born up to the year 2000, the researcher only gathered data on those with a birth date up to 1993, as participants born afterwards would be under the age of 21. Of the 342 participants who accessed the survey, only 171 surveys were accepted, as the remainder were deemed unusable or partially completed and thus were discarded. Data were then brought into MS Excel and converted into SPSS version 23.0. Upon conversion to SPSS, the analysis took place to determine whether a relationship existed between the variables. *QQ* Plots and histograms created for each factor thereby displayed the interval-to-data ratio. Both the *QQ* Plots and the histograms graphically illustrated groups of variable values as intervals (Cooper, 2011). Cronbach's alpha was used to test the internal consistency of each section to determine its reliability; this was followed by a scatter plot that explored the relationship between the two continuous variables. An examination of the two variables was conducted to determine the correlation between them using the Pearson *r* test. Finally, after performing a determination of the relationship between the variables, an *ANOVA* or analysis of variance was performed. The *ANOVA* was used to determine which of the variables had a greater effect on the perceived security awareness level of the participants.

## **Survey Instrument**

The first of two sections contained in the Decker survey instrument contained questions relating to participants' demographic information, and the second section focused on the participants' level of security awareness. The second section consisted of five subsections. The first subsection contained five questions related to internal IT factors. These questions focused on issues such as training and the participants' awareness of the IT security measures found within their organizations. The second subsection posed questions related to internal management factors. The questions asked the participants to express how they perceived management's role in the overall level of security awareness of their organizations. In the third subsection, the participants were asked questions regarding external factors and the influence these factors had on the participants' level of security awareness. The fourth subsection examined inherent factors. It examined the factors that influenced the participants' knowledge regarding, level of interest in, and awareness of information security. The final section asked questions directly related to the security awareness level of the participants and their commitment to the security efforts of their organizations. The Likert scale used a scale from 1 (*strongly disagree*) to 5 (*strongly agree*) and the weighting of each question was equal. The internal consistency of all five sections was tested using Cronbach's alpha in order to determine the degree to which the instrument items were homogeneous and if they reflected equal underlying constructs.

## **Demographics**

The first section provided six demographical questions for the participants to answer. The questions situated the participants' background information and, most importantly, their

generational cohort. The participants' responses were identified and presented in frequency tables.

- Generational cohort: 38.0% of the participants belonged to the Millennial cohort.
- Gender: 50.3% of respondents were male.
- Employment status: 64.3% of the respondents were employed full time.
- Time in organization: 23.4% of respondents had been with their organization between 5 and 15 years.
- Education: 42.1% possessed a bachelor degree.
- Time on computer: 29.8% spent between 51 and 75% of their day on the computer.

The first question identified the generational cohorts the respondents belonged to and provided three possible answers: Baby Boomer, Generation X, or Millennial (Table 5). This information was key to the survey as the focal point of this research was to examine the differences between the generational cohorts. The majority of the respondents were from the Millennial generation at 38.0%, followed closely by the Baby Boomers at 31.6% and Generation X at 30.4%. These results closely followed the intent of the researcher, as the desired outcome was to have 33% from each cohort. The deviation from the researcher's desired outcome was due to the number of discarded responses.

Table 5: Frequency Table - Generational Cohorts

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Baby Boomer	54	31.6	31.6	31.6
	Gen X	52	30.4	30.4	62.0
	Millennial	65	38.0	38.0	100.0
	Total	171	100.0	100.0	

The second demographic question asked the gender of the participants (Table 6). The results from this question were relatively equal with 50.3% male respondents and 49.7% female respondents. While this study did not focus on male-to-female differences, the results were as expected, and a future examination of male-to-female differences in security awareness could be subject to review.

Table 6: Frequency Table - Gender of participant

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	85	49.7	49.7	49.7
	Male	86	50.3	50.3	100.0
	Total	171	100.0	100.0	

The third demographic question asked participants to identify how long they had been with their current organizations or schools. There were six answers available and all received responses. The majority of participants, 64.3%, indicated that they were either full time employees or business owners (Table 7).

Table 7: Frequency Table - Employment/Student status

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Employed Full time or business owner	110	64.3	64.3	64.3
	Employed Part time	16	9.4	9.4	73.7
	Full time student	13	7.6	7.6	81.3
	Part time student	2	1.2	1.2	82.5
	Retired	19	11.1	11.1	93.6
	Disabled	11	6.4	6.4	100.0
	Total	171	100.0	100.0	

The purpose of the third demographic question was to determine the duration of the employment or student status of the employees or students at their organizations or schools

(Table 8). This question presented six possible categories, with all six categories receiving responses. The largest number of respondents were found in the 5 - 15 year range with 23.4% of the respondents, followed by the 1 – 3 year range with 19.9%, and then by 19.3% who indicated they had been with their organization/school less than a year.

Table 8: Frequency table - Years of employment/at school

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 1 yr	33	19.3	19.3	19.3
	1 to 3 yrs	34	19.9	19.9	39.2
	3 to 5 yrs	24	14.0	14.0	53.2
	5 to 15 yrs	40	23.4	23.4	76.6
	15 to 25 yrs	21	12.3	12.3	88.9
	Over 25 yrs	19	11.1	11.1	100.0
	Total	171	100.0	100.0	

The fifth demographical question examined the highest level of education of the participants (Table 9). All six possible answers received responses. The majority of participants, or 42.1%, possessed a bachelor's degree, followed by possession of a graduate degree at 26.9%, and some college but no degree at 15.8%.

Table 9: Frequency table - Level of education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than HS	1	.6	.6	.6
	HS or Equiv	13	7.6	7.6	8.2
	Some college, no degree	27	15.8	15.8	24.0
	Associate degree	12	7.0	7.0	31.0
	Bachelor degree	72	42.1	42.1	73.1
	Graduate degree	46	26.9	26.9	100.0
	Total	171	100.0	100.0	

The sixth and final demographic question asked respondents to indicate the percentage of their day spent on the computer (Table 10). All five categories received responses. The category

receiving the most responses was 51-75% of their day, which accounted for 29.8% of responses. This was followed by 26-50% of their day for 25.7% of respondents, and 1-25% of their day for 23.4% of respondents.

Table 10: Frequency table - Percentage of day spend on the computer

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0%	5	2.9	2.9	2.9
	1-25%	40	23.4	23.4	26.3
	26-50%	44	25.7	25.7	52.0
	51-75%	51	29.8	29.8	81.9
	76-100%	31	18.1	18.1	100.0
	Total	171	100.0	100.0	

### Security Awareness

The second portion of the Decker survey instrument (2008) looked at how the independent variables in the study, internal IT factors, internal management factors, external factors, and inherent factors, affected the participants' perceived levels of security awareness. The survey instrument was employed to define which of the independent variables had the greatest effect on the participants' overall security awareness level. Each factor was examined and a histogram was presented to display the results. This displayed the distribution of scores on the continuous variable (Stokes, 2011). The sections were then examined for internal consistency using Cronbach's alpha.

The responses in each section were given a value on the Likert scale from 1 to 5, with 1 indicating *strong disagreement* and 5 *strong agreement*. Each response in the security awareness section was assessed from the lowest possible score of 5 to the maximum score of 25. The histogram then provided a depiction of how the respondents answered and the distribution of their responses. The questions were weighted equally in all subsections.

## Internal IT Factors

The first subsection, Internal IT Factors, examined all generational cohorts using five questions to determine the familiarity of the participants with their organizations' acceptable use policies and their requirement to complete security awareness training in the workplace. A *QQ* Plot (Figure A1) and a histogram indicated a normal distribution with a mean of 18.23 and a standard deviation of 5.089 (Figure A2). Eight participants (4.7%) answered with a minimum score of 5 and 23 participants (13.5%) replied with the maximum score of 25. Cronbach's alpha examined the internal consistency for internal IT factors for all generational cohorts with a score of 0.874, indicating a good level of internal consistency (Table A1).

Baby Boomer results were examined with the results of the *QQ* Plot (Figure A3) and histogram indicating a normal distribution with a mean of 18.46 and a standard deviation of 5.393 (Figure A4). Three participants (5.6%) answered with a minimum score of five, and eight participants (14.8%) replied with the maximum score of 25. Generation X cohort data were extracted for examination and the results of the *QQ* Plot (Figure A5) and histogram indicated a normal distribution with a mean of 19.19 and a standard deviation of 4.678 (Figure A6). One participant (1.9%) answered with a minimum score of five, and ten participants (19.2%) replied with the maximum score of 25. Finally, the Millennials' data were then extracted for examination and the results of the *QQ* Plot (Figure A7) and histogram indicated a normal distribution with a mean of 17.28 and a standard deviation of 5.054 (Figure A8). Four participants (6.2%) answered with a minimum score of five, and five participants (14.8%) replied with the maximum score of 25.



## **Internal Management Factors**

The second subsection, Internal Management Factors, examined all generational cohorts using six questions to determine their perception of management's role in the level of security awareness of their organizations. A *QQ* Plot (Figure A9) and a histogram indicated a normal distribution with a mean of 18.60 and a standard deviation of 5.427 (Figure A10). Six participants (3.5%) answered with a minimum score of six, and four participants (2.3%) replied with the maximum score of 30. Cronbach's alpha examined the internal consistency for internal management factors for all generational cohorts, resulting in a score of 0.849, indicating a good level of internal consistency (Table A2).

Baby Boomer results were extracted with the results of the *QQ* Plot (Figure A11) and histogram, indicating a normal distribution with a mean of 17.91 and a standard deviation of 5.577 (Figure A12). Two participants (3.7%) answered with a minimum score of six, and one participant (1.9%) replied with the maximum score of 30. Generation X cohort data were extracted and the results of the *QQ* Plot (Figure A13) and histogram indicated a normal distribution with a mean of 18.83 and a standard deviation of 4.63 (Figure A14). One participant (1.9%) answered with a minimum score of six, and two participants (3.7%) replied with the maximum score of 30. Finally, the Millennials' data were then extracted and the results of the *QQ* Plot (Figure A15) and histogram indicated a normal distribution with a mean of 19.00 and a standard deviation of 5.874 (Figure A16). Four participants (6.2%) answered with a minimum score of six, and three participants (4.6%) replied with the maximum score of 30.

## **External Factors**

The third subsection, External Factors, examined all generational cohorts using five questions to determine the role external factors possessed in the level of security awareness of

their organizations. A *QQ* Plot (Figure A17) and a histogram indicated a normal distribution with a mean of 18.22 and a standard deviation of 3.753 (Figure A18). Three participants (1.8%) answered with a minimum score of five and nine participants (5.3%) replied with the maximum score of 25. Cronbach's alpha examined the internal consistency for external factors for all generational cohorts, resulting in a score of 0.643, indicating an acceptable level of internal consistency (Table A3).

Baby Boomer results were extracted with the results of the *QQ* Plot (Figure A19) and histogram indicating a normal distribution with a mean of 18.31 and a standard deviation of 4.009 (Figure A20). One participant (1.9%) answered with a minimum score of five, and four participants (7.4%) replied with the maximum score of 25. Generation X cohort data were extracted and the results of the *QQ* Plot (Figure A21) and histogram indicated a normal distribution with a mean of 18.31 and a standard deviation of 2.954 (Figure A22). One participant (1.9%) answered with a minimum score of five, and one participant (1.9%) replied with the maximum score of 25. Finally, the Millennials' data were then extracted and the results of the *QQ* Plot (Figure A23) and histogram indicated a normal distribution with a mean of 18.06 and a standard deviation of 4.138 (Figure A24). Two participants (3.1%) answered with a minimum score of five, and five participants (7.7%) replied with the maximum score of 25.

### **Inherent Factors**

The fourth subsection, Inherent Factors, examined all generational cohorts and the participants' knowledge of, level of interest in, and awareness of information security. A *QQ* Plot (Figure A25) and a histogram indicated a normal distribution with a mean of 17.80 and a standard deviation of 3.562 (Figure A26). Two participants (1.2%) answered with a minimum score of five and four participants (2.3%) replied with the maximum score of 25. Cronbach's

alpha examined the internal consistency for inherent factors for all generational cohorts, resulting in a score of 0.682, indicating an acceptable level of internal consistency (Table A4).

Baby Boomer results were extracted with the results of the *QQ* Plot (Figure A27) and histogram indicating a normal distribution with a mean of 17.89 and a standard deviation of 3.638 (Figure A28). One participant (1.9%) answered with a minimum score of five and one participant (1.9%) replied with the maximum score of 25. Generation X cohort data were extracted and the results of the *QQ* Plot (Figure A29) and histogram indicated a normal distribution with a mean of 18.00 and a standard deviation of 2.849 (Figure A30). One participant (1.9%) answered with a minimum score of five, and one participant (1.9%) replied with the maximum score of 25. Finally, the Millennials' data were then extracted and the results of the *QQ* Plot (Figure A31) and histogram indicated a normal distribution with a mean of 17.57 and a standard deviation of 4.023 (Figure A32). Two participants (3.1%) answered with a minimum score of five, and three participants (4.6%) replied with the maximum score of 25.

### **Perceived Security Awareness Level**

The fifth and final subsection, Inherent Factors, examined all generational cohorts and contained four questions related to the security awareness level of the participants and their commitment to the security efforts of their organizations. A *QQ* Plot (Figure A33) and a histogram indicated a normal distribution with a mean of 14.98 and a standard deviation of 3.137 (Figure A34). Two participants (1.2%) answered with a minimum score of four and sixteen participants (9.4%) replied with the maximum score of sixteen. Cronbach's alpha examined the internal consistency for internal management factors for all generational cohorts, resulting in a score of 0.767, indicating a good level of internal consistency (Table A5).

Baby Boomer results were extracted with the results of the *QQ* Plot (Figure A35) and histogram indicating a normal distribution with a mean of 15.19 and a standard deviation of 3.066 (Figure A36). Two participants (1.2%) answered with a minimum score of four, and six participants (11.1%) replied with the maximum score of sixteen. Generation X cohort data were extracted and the results of the *QQ* Plot (Figure A37) and histogram indicated a normal distribution with a mean of 15.52 and a standard deviation of 2.653 (Figure A38). One participant (1.9%) answered with a minimum score of four, and five participants (9.6%) replied with the maximum score of sixteen. Finally, the Millennials' data were then extracted and the results of the *QQ* Plot (Figure A39) and histogram indicated a normal distribution with a mean of 14.38 and a standard deviation of 3.481 (Figure A40). Two participants (3.1%) answered with a minimum score of four, and five participants (9.6%) replied with the maximum score of sixteen.

### **Hypothesis Results**

This section analyzes the four independent variables, internal IT, internal management, external, and inherent factors, and their correlation with the dependent variable, perceived security awareness level. This process was repeated for each generational cohort being studied, the Baby Boomer, Generation X, and Millennial generations. The relationship between the two continuous variables was examined using a scatter plot to visually demonstrate the linear relationship and the strength of the relationship between the variables (Cooper, 2011). Once linearity was positively established using the scatter plot, a Pearson *r* was run, which analyzed the relationship between the variables. Once the strength of the relationship between the variables was determined, an *ANOVA* was used to determine whether the means were significantly different from each other.

### **Hypothesis 1: Internal IT Factors (security awareness training)**

H<sub>101</sub> = Internal IT factors are not significantly related to the perceived security awareness level of end users of the Baby Boomer generation.

H<sub>101</sub> considered the relationship between the internal IT factors and the participants' perceived cyber security awareness levels for the Baby Boomer generational cohort. The questions related to internal IT factors asked Baby Boomer participants whether they had taken any formal security awareness training and asked other, similar questions that examined their knowledge of security awareness learned either formally or informally.

A scatter plot was used to determine the relationship between the two continuous variables, internal IT factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between internal IT factors and the level of perceived security awareness of the Baby Boomer participants with number of outliers (Figure 22). Upon establishing the existence of a possible positive correlation through the scatter plot, the Pearson  $r$  bivariate correlation coefficient was computed to assess the relationship between the internal IT factors and the level of perceived security awareness. The Pearson  $r$  bivariate correlation indicated that there existed a weak correlation between variables with  $r = 0.645$ ,  $n = 54$ , and  $p = 0.000$  (Table 11). The significance value was .000, indicating that a significance existed; therefore, the null hypothesis H<sub>101</sub> could be rejected. Further exploration of the significance of variables was conducted with an *ANOVA* (Table 12), indicating that a significant difference existed as  $p = .000$  ( $p < .050$ ).

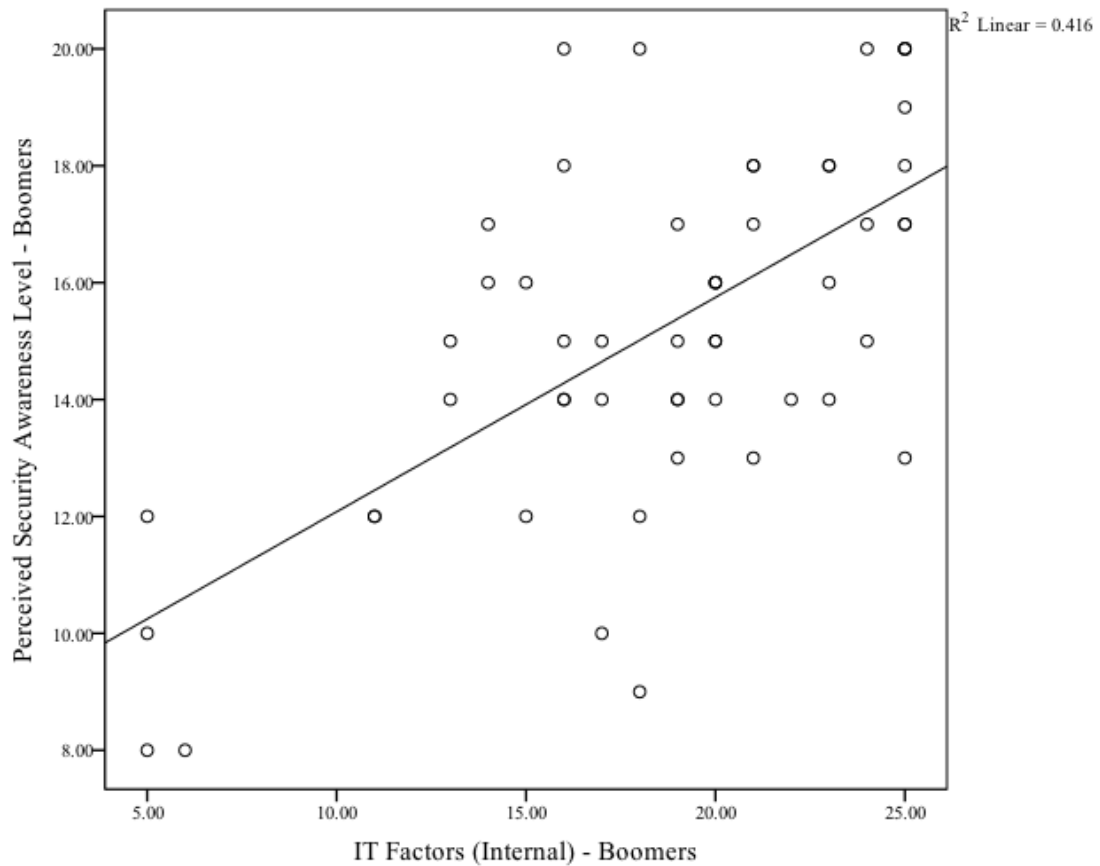


Figure 2: Scatter plot - Internal IT Factors (Baby Boomer)

Table 11: Pearson Correlation - Internal IT Factors (Baby Boomer)

		Internal IT	Perceived
Internal IT	Pearson Correlation	1	.645**
	Sig. (2-tailed)		.000
	<i>N</i>	54	54
Perceived	Pearson Correlation	.645**	1
	Sig. (2-tailed)	.000	
	<i>N</i>	54	54

\*\* Correlation is significant at the 0.01 level (2-tailed).

Table 12: *ANOVA* - Internal IT Factors (Baby Boomer)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	917.545	11	83.413	5.615	.000
Within Groups	623.881	42	14.854		
Total	1541.426	53			

H1<sub>02</sub> = Internal IT factors are not significantly related to the perceived security awareness level of end users of the Gen X generation.

H1<sub>02</sub> considered the relationship between internal IT factors and the participants' perceived cyber security awareness levels for the Gen X generational cohort. The questions related to internal IT factors asked Gen X participants whether they had taken any formal security awareness training and asked other, similar questions that examined their knowledge of security awareness learned either formally or informally.

A scatter plot was used to determine the relationship between the two continuous variables, internal IT factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between internal IT factors and the level of perceived security awareness of the Gen X participants with number of outliers (Figure 23). Upon establishing the existence of a linear relationship through the scatter plot, the Pearson *r* bivariate correlation coefficient was computed to assess the relationship between the internal IT factors and the level of perceived security awareness. The Pearson *r* bivariate correlation indicated that there existed a weak correlation between variables with  $r = 0.532$ ,  $n = 52$ , and  $p = 0.000$  (Table 13). The significance value was .000, indicating that a strong significance existed; therefore, the null hypothesis H1<sub>02</sub> could be rejected. Further exploration of the significance of variables was conducted with an *ANOVA* (Table 14), indicating that a significant difference existed as  $p = .042$  ( $p < .050$ ).

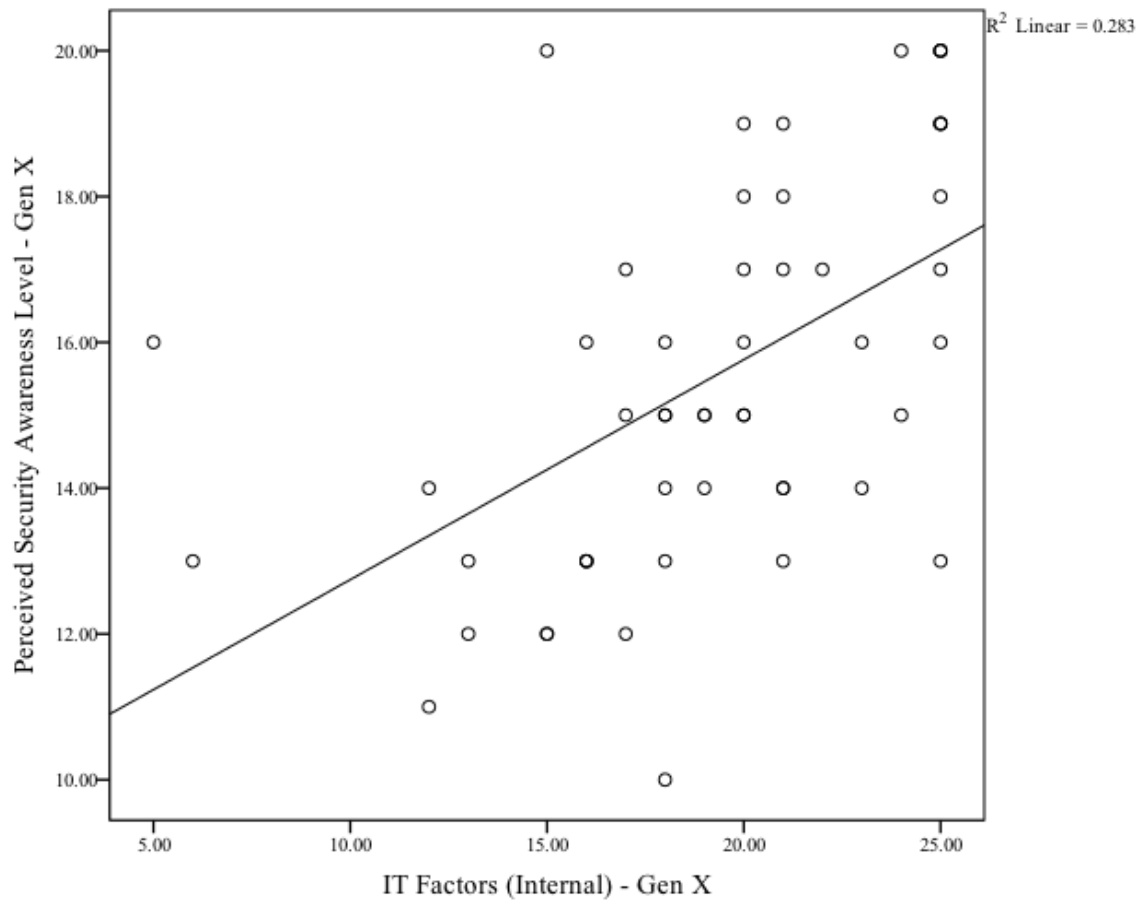


Figure 3: Scatter plot - Internal IT Factors (Generation X)

Table 13: Pearson Correlation - Internal IT Factors (Generation X)

		Perceived	Internal IT
Perceived	Pearson Correlation	1	.532**
	Sig. (2-tailed)		.000
	<i>N</i>	52	52
Internal IT	Pearson Correlation	.532**	1
	Sig. (2-tailed)	.000	
	<i>N</i>	52	52

\*\* Correlation is significant at the 0.01 level (2-tailed).



Table 14: *ANOVA* - Internal IT Factors (Generation X)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	383.894	10	38.389	2.150	.042
Within Groups	732.183	41	17.858		
Total	1116.077	51			

H<sub>103</sub> = Internal IT factors are not significantly related to the perceived security awareness level of end users of the Millennial generation.

H<sub>103</sub> considered the relationship between internal IT factors and the participants' perceived cyber security awareness levels for the Millennial generational cohort. The questions related to internal IT factors asked Millennial participants whether they had taken any formal security awareness training and asked other, similar questions that examined their knowledge of security awareness learned either formally or informally.

A scatter plot was used to determine the relationship between the two continuous variables, internal IT factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between internal IT factors and the level of perceived security awareness of the Millennial participants with number of outliers (Figure 24). Upon establishing the existence of a linear relationship through the scatter plot, the Pearson *r* bivariate correlation coefficient was computed to assess the relationship between the Internal IT Factors and the level of perceived security awareness. The Pearson *r* bivariate correlation indicated that there existed a weak correlation between variables with  $r = 0.664$ ,  $n = 65$ , and  $p = 0.000$  (Table 15). The significance value was .000, indicating that a strong significance existed; therefore, the null hypothesis H<sub>103</sub> could be rejected. Further exploration of the significance of variables was

conducted with an *ANOVA* (Table 16), indicating that a significant difference existed as  $p = .000$  ( $p < .050$ ).

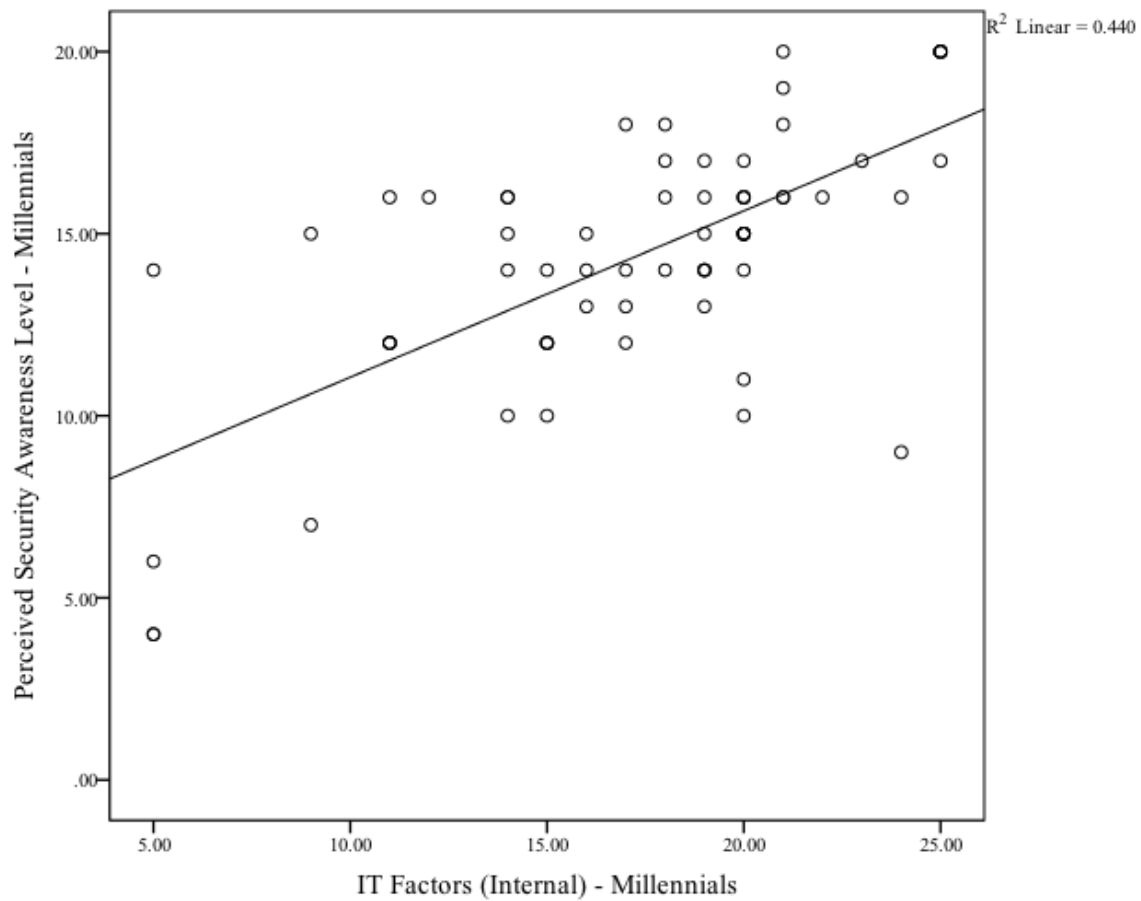


Figure 4: Scatter plot - Internal IT Factors (Millennial)

Table 15: Pearson Correlation - Internal IT Factors (Millennial)

		Internal IT	Perceived
Internal IT	Pearson Correlation	1	.664**
	Sig. (2-tailed)		.000
	<i>N</i>	65	65
Perceived	Pearson Correlation	.664**	1
	Sig. (2-tailed)	.000	
	<i>N</i>	65	65

\*\* Correlation is significant at the 0.01 level (2-tailed).

Table 16: *ANOVA* - Internal IT Factors (Millennial)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	1022.987	14	73.070	5.970	.000
Within Groups	612.029	50	12.241		
Total	1635.015	64			

## Hypothesis 2: Internal Management Factors

H2<sub>01</sub> = Internal management factors are not significantly related to the perceived security awareness level of end users of the Baby Boomer generation.

H2<sub>01</sub> considered the relationship between internal management factors and the participants' perceived cyber security awareness levels for the Baby Boomer generational cohort. The questions related to internal management factors asked Baby Boomer participants whether they found management's dedication to cyber security awareness sufficient, whether regular security awareness training was provided, and if participants understood the penalties for security breaches.

A scatter plot was used to determine the relationship between the two continuous variables, internal management factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between internal management factors and the level of perceived security awareness of the Baby Boomer participants with number of outliers (Figure 25). Upon establishing the existence of a linear relationship through the scatter plot, the Pearson *r* bivariate correlation coefficient was computed to assess the relationship between internal management factors and the level of perceived security awareness. The Pearson *r* bivariate correlation indicated that there existed a strong correlation between variables with  $r = 0.702$ ,  $n =$

54, and  $p = 0.000$  (Table 17). The significance value was .000, indicating that a strong significance existed; therefore, the null hypothesis H2<sub>01</sub> could be rejected. Further exploration of the significance of variables was conducted with an *ANOVA* (Table 18), indicating that a significant difference existed as  $p = .000$  ( $p < .050$ ).

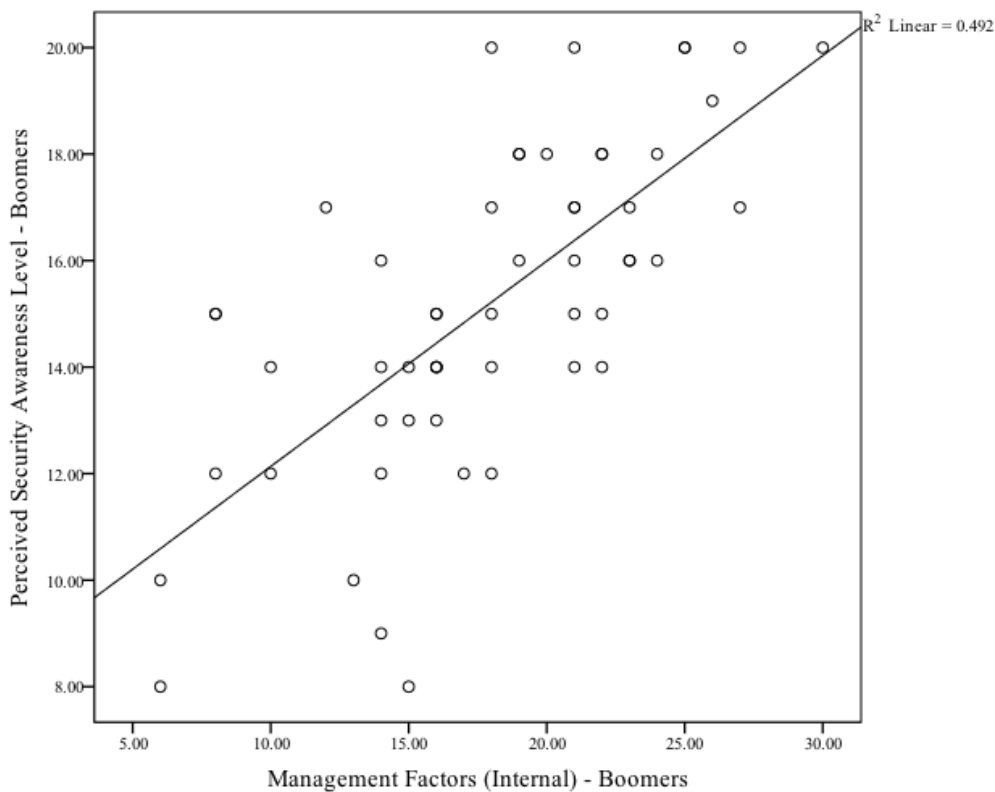


Figure 5: Scatter plot - Internal Management Factors (Baby Boomer)

Table 17: Pearson Correlation - Internal Management Factors (Baby Boomer)

		Perceived	Management
Perceived	Pearson Correlation	1	.702**
	Sig. (2-tailed)		.000
	<i>N</i>	54	54
Management	Pearson Correlation	.702**	1
	Sig. (2-tailed)	.000	
	<i>N</i>	54	54

\*\* Correlation is significant at the 0.01 level (2-tailed).

Table 18: *ANOVA* - Internal Management Factors (Baby Boomer)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	902.401	11	82.036	4.618	.000
Within Groups	746.137	42	17.765		
Total	1648.537	53			

H2<sub>02</sub> = Internal management factors are not significantly related to the perceived security awareness level of end users of the Gen X generation.

H2<sub>02</sub> considered the relationship between internal management factors and the participants' perceived cyber security awareness levels for the Gen X generational cohort. The questions related to internal management factors asked Gen X participants whether they found management's dedication to cyber security awareness sufficient, whether regular security awareness training was provided, and if participants understood the penalties for security breaches.

A scatter plot was used to determine the relationship between the two continuous variables, internal management factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between internal management factors and the level of perceived security awareness of the Gen X participants with number of outliers (Figure 26). Upon establishing the existence of a linear relationship through the scatter plot, the Pearson *r* bivariate correlation coefficient was computed to assess the relationship between internal management factors and the level of perceived security awareness. The Pearson *r* bivariate correlation indicated that there existed a weak correlation between variables with  $r = 0.592$ ,  $n = 52$ , and  $p = 0.000$  (Table 19). The significance value was .000, indicating that a strong significance existed; therefore, the null hypothesis H2<sub>02</sub> could be rejected. Further exploration

of the significance of variables was conducted with an *ANOVA* (Table 20), indicating that a significant difference existed as  $p = .009$  ( $p < .050$ ).

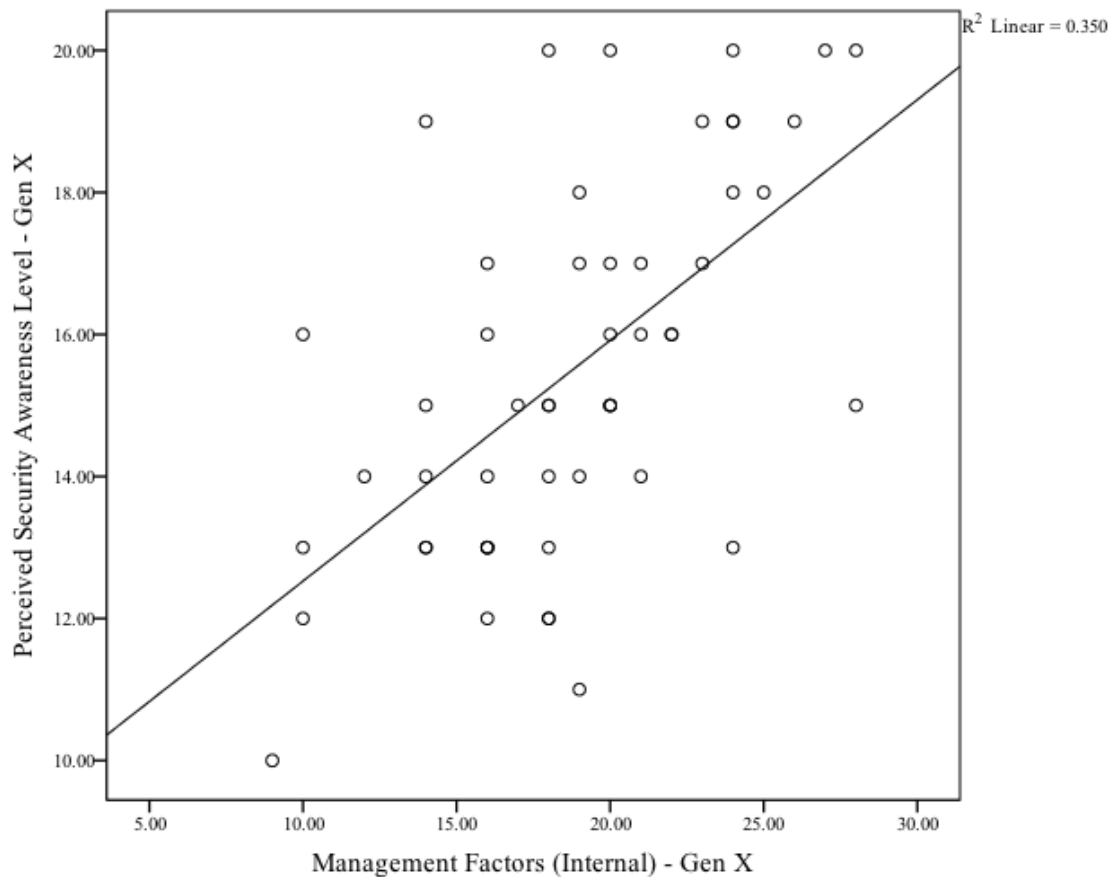


Figure 6: Scatter plot - Internal Management Factors (Generation X)

Table 19: Pearson Correlation - Internal Management Factors (Generation X)

		Perceived	Management
Perceived	Pearson Correlation	1	.592**
	Sig. (2-tailed)		.000
	<i>N</i>	52	52
Management	Pearson Correlation	.592**	1
	Sig. (2-tailed)	.000	
	<i>N</i>	52	52

\*\* Correlation is significant at the 0.01 level (2-tailed).

Table 20: *ANOVA* - Internal Management Factors (Generation X)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	446.267	10	44.627	2.827	.009
Within Groups	647.175	41	15.785		
Total	1093.442	51			

H2<sub>03</sub> = Internal management factors are not significantly related to the perceived security awareness level of end users of the Millennial generation.

H2<sub>03</sub> considered the relationship between internal management factors and the participants' perceived cyber security awareness levels for the Millennial generational cohort. The questions related to internal management factors asked Millennial participants whether they found management's dedication to cyber security awareness sufficient, whether regular security awareness training was provided, and if participants understood the penalties for security breaches.

A scatter plot was used to determine the relationship between the two continuous variables, internal management factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between internal management factors and the level of perceived security awareness of the Millennial participants with number of outliers (Figure 27). Upon establishing the existence of a linear relationship through the scatter plot, the Pearson *r* bivariate correlation coefficient was computed to assess the relationship between internal management factors and the level of perceived security awareness. The Pearson *r* bivariate correlation indicated that there existed a weak correlation between variables with  $r = 0.660$ ,  $n = 65$ , and  $p = 0.000$  (Table 21). The significance value was .000, indicating that a strong significance existed; therefore, the null hypothesis H2<sub>03</sub> could be rejected. Further exploration

of the significance of variables was conducted with an *ANOVA* (Table 22), indicating that a significant difference existed as  $p = .000$  ( $p < .050$ ).

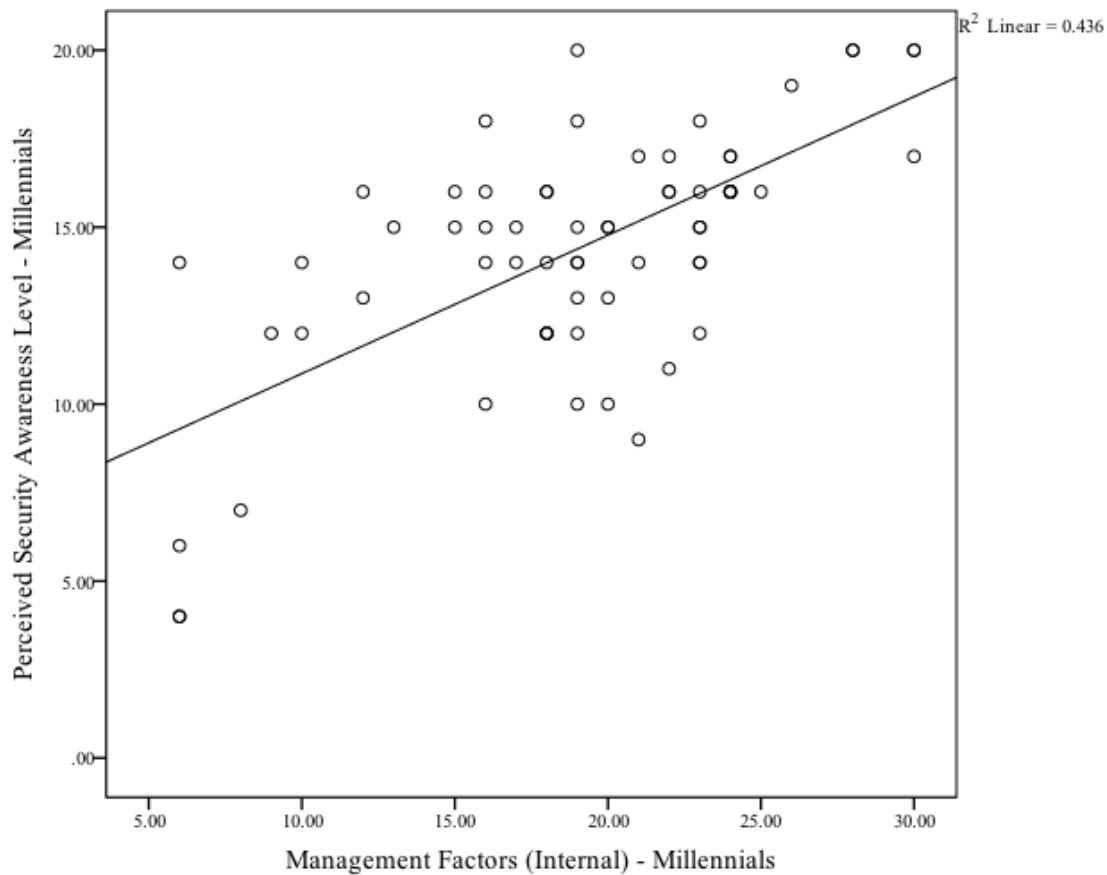


Figure 7: Scatter plot - Internal Management Factors (Millennial)

Table 21: Pearson Correlation - Internal Management Factors (Millennial)

		Perceived	Management
Perceived	Pearson Correlation	1	.660**
	Sig. (2-tailed)		.000
	<i>N</i>	65	65
Management	Pearson Correlation	.660**	1
	Sig. (2-tailed)	.000	
	<i>N</i>	65	65

\*\* Correlation is significant at the 0.01 level (2-tailed).



Table 22: ANOVA - Internal Management Factors (Millennial)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	1271.099	14	90.793	4.845	.000
Within Groups	936.901	50	18.738		
Total	2208.000	64			

### Hypothesis 3: External Factors

H<sub>301</sub> = External factors are not significantly related to the perceived security awareness level of end users of the Baby Boomer generation.

H<sub>301</sub> considered the relationship between external factors and the participants' perceived cyber security awareness levels for the Baby Boomer generational cohort. The questions related to external factors asked Baby Boomer participants whether they were aware of current world events related to cyber security, governmental requirements, and news regarding cyber security incidents, or if they regularly received material regarding information security from their financial institutions.

A scatter plot was used to determine the relationship between the two continuous variables, external factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between external factors and the level of perceived security awareness of the Baby Boomer participants with number of outliers (Figure 28). Upon establishing the existence of a linear relationship through the scatter plot, the Pearson *r* bivariate correlation coefficient was computed to assess the relationship between external factors and the level of perceived security awareness. The Pearson *r* bivariate correlation indicated that there existed a weak correlation between variables with  $r = 0.558$ ,  $n = 54$ , and  $p = 0.000$  (Table 23). The significance value was .002, indicating that a strong significance existed; therefore, the null

hypothesis H3<sub>01</sub> could be rejected. Further exploration of the significance of variables was conducted with an ANOVA (Table 24), indicating that a significant difference existed as  $p = .002$  ( $p < .050$ ).

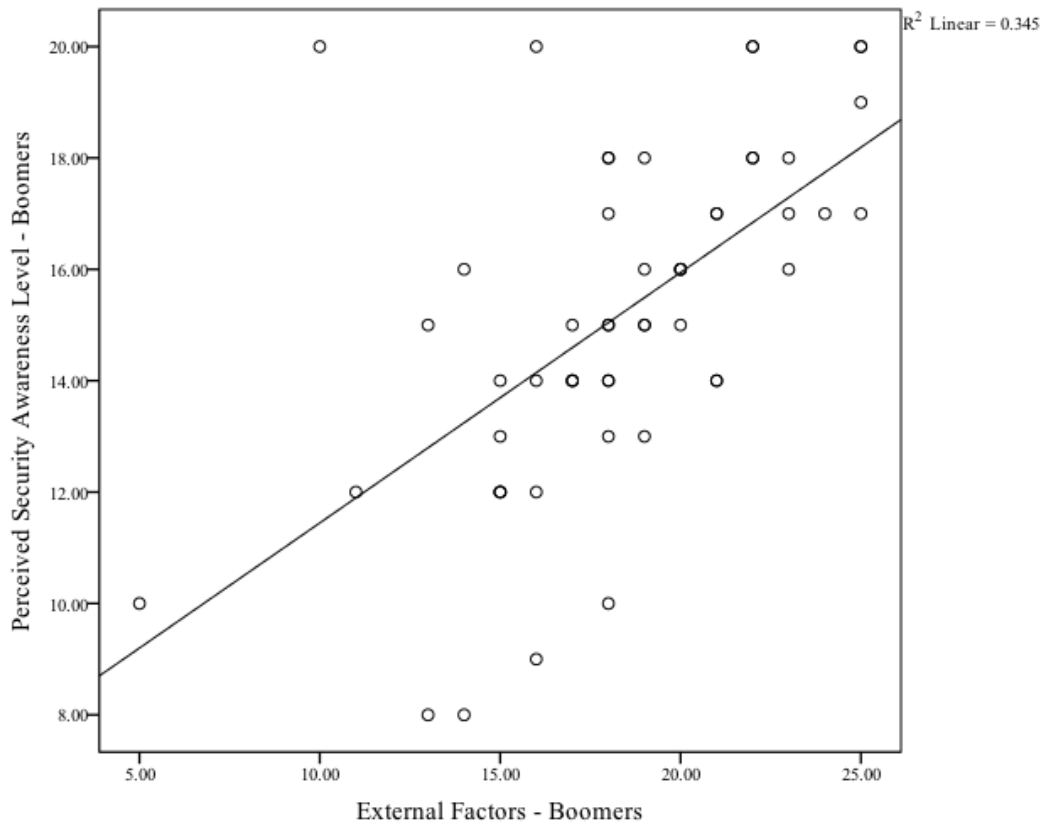


Figure 8: Scatter plot - External Factors (Baby Boomer)

Table 23: Pearson Correlation - External Factors (Baby Boomer)

		Perceived	External
Perceived	Pearson Correlation	1	.588**
	Sig. (2-tailed)		.000
	<i>N</i>	54	54
External	Pearson Correlation	.588**	1
	Sig. (2-tailed)	.000	
	<i>N</i>	54	54

\*\* Correlation is significant at the 0.01 level (2-tailed).

Table 24: *ANOVA* - External Factors (Baby Boomer)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	403.131	11	36.648	3.432	.002
Within Groups	448.517	42	10.679		
Total	851.648	53			

H3<sub>02</sub> = External factors are not significantly related to the perceived security awareness level of end users of the Gen X generation.

H3<sub>02</sub> considered the relationship between external factors and the participants' perceived cyber security awareness levels for the Gen X generational cohort. The questions related to external factors asked Gen X participants whether they were aware of current world events related to cyber security, governmental requirements, and news regarding cyber security incidents, and if they had regularly received material regarding information security from their financial institution.

A scatter plot was used to determine the relationship between the two continuous variables, external factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between external factors and the level of perceived security awareness of the Gen X participants with number of outliers (Figure 29). Upon establishing the existence of a linear relationship through the scatter plot, the Pearson *r* bivariate correlation coefficient was computed to assess the relationship between external factors and the level of perceived security awareness. The Pearson *r* bivariate correlation indicated that there existed a weak correlation between variables with  $r = 0.605$ ,  $n = 52$ , and  $p = 0.000$  (Table 25). The significance value was .003, indicating that a strong significance existed; therefore, the null hypothesis H3<sub>02</sub> could be rejected. Further exploration of the significance of variables was

conducted with an *ANOVA* (Table 26), indicating a significant difference existed as  $p = .003$  ( $p < .050$ ).

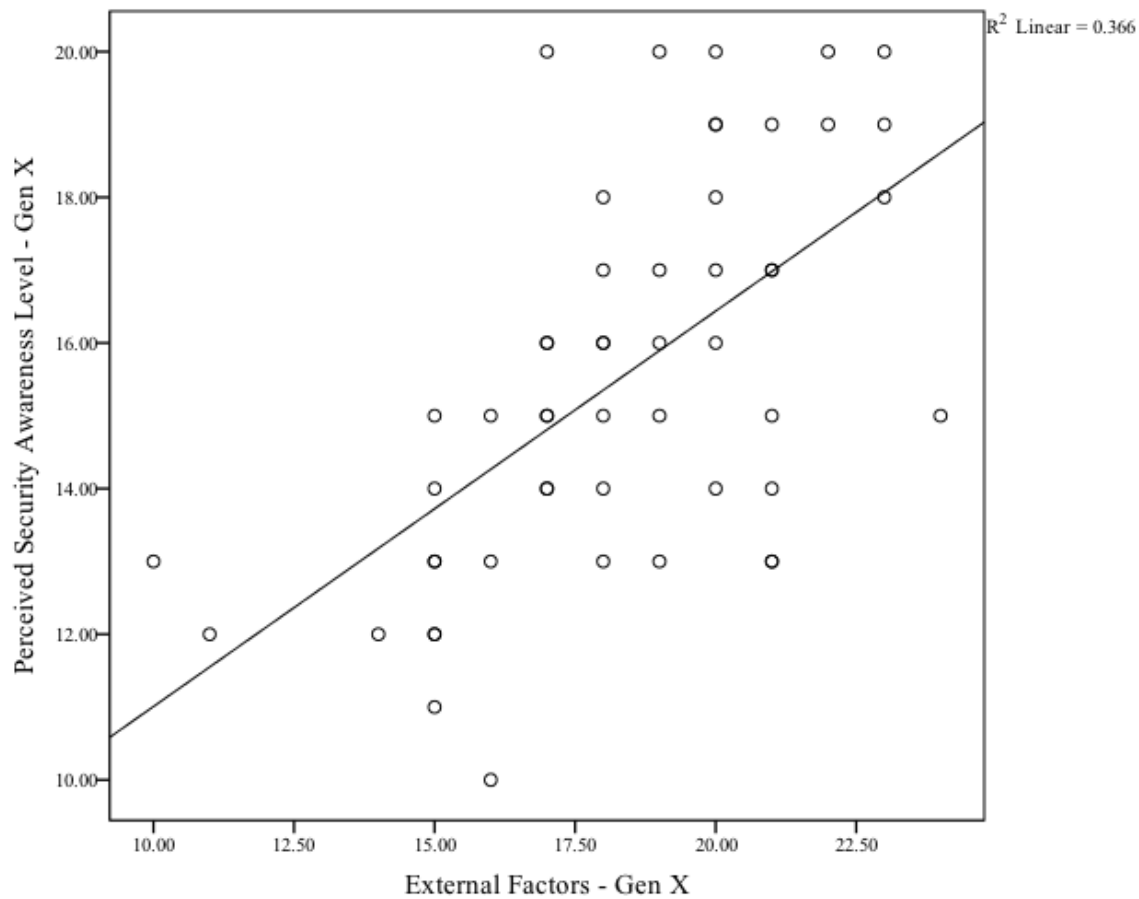


Figure 9: Scatter plot - External Factors (Generation X)

Table 25: Pearson Correlation - External Factors (Generation X)

		Perceived	External
Perceived	Pearson Correlation	1	.605**
	Sig. (2-tailed)		.000
	N	52	52
External	Pearson Correlation	.605**	1
	Sig. (2-tailed)	.000	
	N	52	52

\*\* Correlation is significant at the 0.01 level (2-tailed).

Table 26: *ANOVA* - External Factors (Generation X)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	199.677	10	19.968	3.336	.003
Within Groups	245.400	41	5.985		
Total	445.077	51			

H3<sub>03</sub> = External factors are not significantly related to the perceived security awareness level of end users of the Millennial generation.

H3<sub>03</sub> considered the relationship between external factors and the participants' perceived cyber security awareness levels for the Millennial generational cohort. The questions related to external factors asked Millennial participants whether they were aware of current world events related to cyber security, governmental requirements, and news regarding cyber security incidents, and if they had regularly received material regarding information security from their financial institution.

A scatter plot was used to determine the relationship between the two continuous variables, external factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between external factors and the level of perceived security awareness of the Millennial participants with number of outliers (Figure 30). Upon establishing the existence of a linear relationship through the scatter plot, the Pearson *r* bivariate correlation coefficient was computed to assess the relationship between internal management factors and the level of perceived security awareness. The Pearson *r* bivariate correlation indicated that there existed a weak correlation between variables with  $r = 0.625$ ,  $n = 65$ , and  $p = 0.000$  (Table 27). The significance value was .000, indicating that a strong significance existed; therefore, the null hypothesis H3<sub>03</sub> could be rejected. Further exploration of the significance of variables was

conducted with an *ANOVA* (Table 28), indicating that a significant difference existed as  $p = .000$  ( $p < .050$ ).

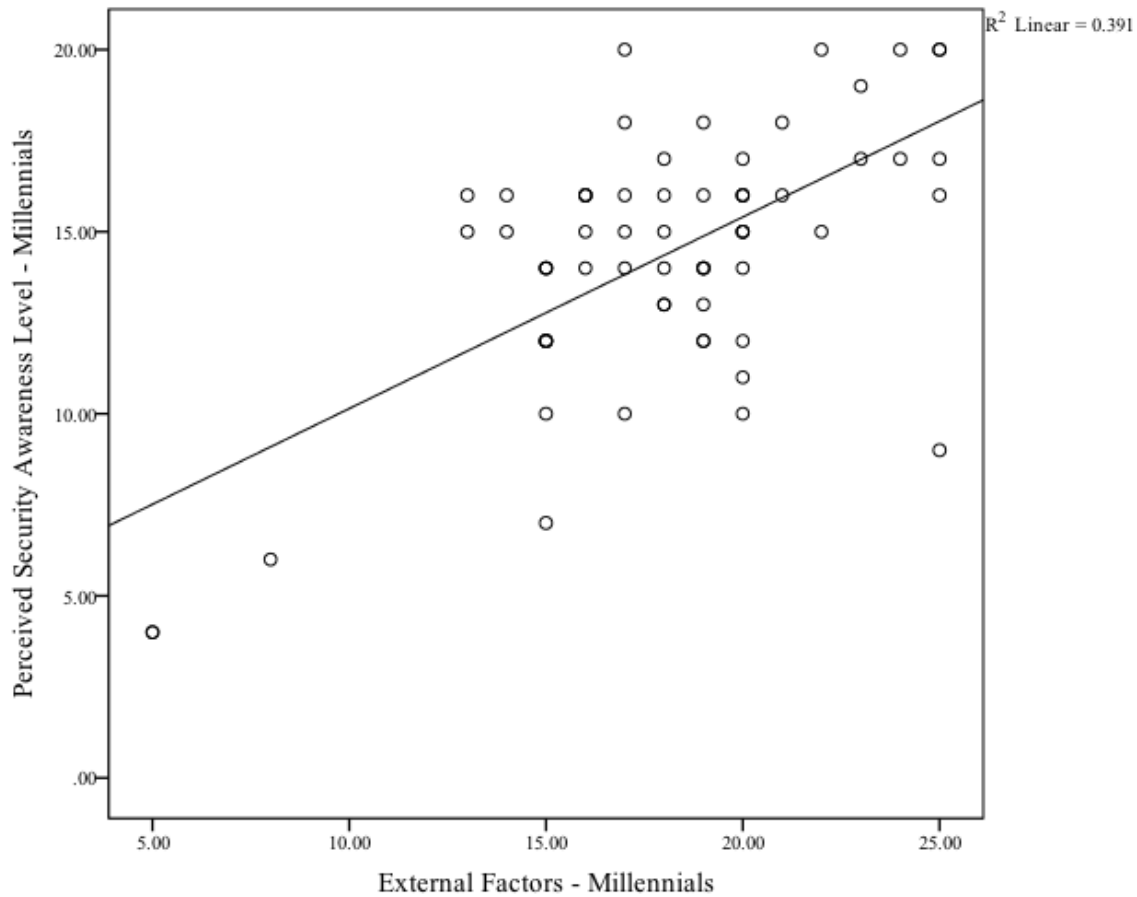


Figure 10: Scatter plot - External Factors (Millennial)

Table 27: Pearson Correlation - External Factors (Millennial)

		Perceived	External
Perceived	Pearson Correlation	1	.625**
	Sig. (2-tailed)		.000
	<i>N</i>	65	65
External	Pearson Correlation	.625**	1
	Sig. (2-tailed)	.000	
	<i>N</i>	65	65

\*\* Correlation is significant at the 0.01 level (2-tailed).

Table 28: *ANOVA* - External Factors (Millennial)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	729.785	14	52.127	7.122	.000
Within Groups	365.969	50	7.319		
Total	1095.754	64			

#### Hypothesis 4: Inherent Factors

H<sub>401</sub> = Inherent factors are not significantly related to the perceived security awareness level of end users of the Baby Boomer generation.

H<sub>401</sub> considered the relationship between inherent factors and the participants' perceived cyber security awareness levels for the Baby Boomer generational cohort. The questions related to inherent factors were generally an examination of the Baby Boomer participants' personal factors, such as their interest in participating in training, their knowledge level, and the value they placed on cyber security within their organizations.

A scatter plot was used to determine the relationship between the two continuous variables, inherent factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between inherent factors and the level of perceived security awareness of the Baby Boomer participants with number of outliers (Figure 31). Upon establishing the existence of a linear relationship through the scatter plot, the Pearson *r* bivariate correlation coefficient was computed to assess the relationship between inherent factors and the level of perceived security awareness. The Pearson *r* bivariate correlation indicated that there existed a weak correlation between variables with  $r = 0.613$ ,  $n = 54$ , and  $p = 0.000$  (Table 29). The significance value was .000, indicating that a strong significance existed; therefore, the null hypothesis H<sub>401</sub> could be rejected. Further exploration of the significance of variables was

conducted with an *ANOVA* (Table 30), indicating that a significant difference existed as  $p = .000$  ( $p < .050$ ).

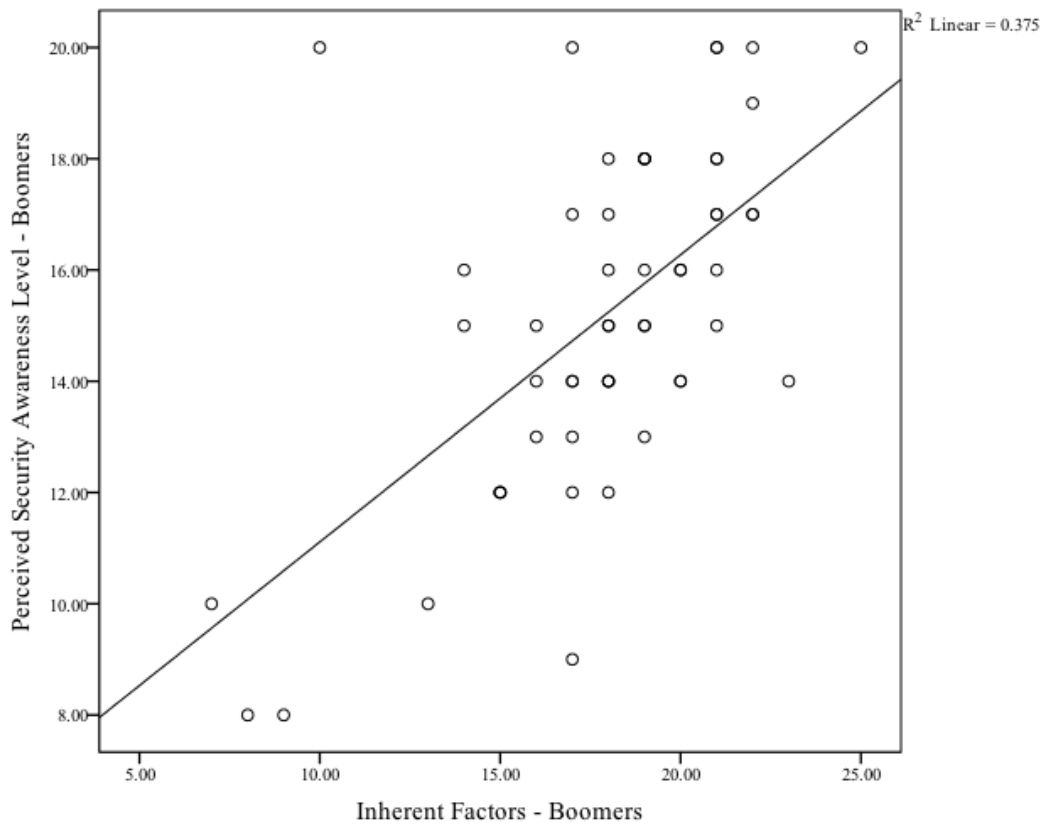


Figure 11: Scatter plot - Inherent Factors (Baby Boomer)

Table 29: Pearson Correlation - Inherent Factors (Baby Boomer)

		Perceived	Inherent
Perceived	Pearson Correlation	1	.613**
	Sig. (2-tailed)		.000
	<i>N</i>	54	54
Inherent	Pearson Correlation	.613**	1
	Sig. (2-tailed)	.000	
	<i>N</i>	54	54

\*\* Correlation is significant at the 0.01 level (2-tailed).



Table 30: *ANOVA* - Inherent Factors (Baby Boomer)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	404.087	11	36.735	5.191	.000
Within Groups	297.246	42	7.077		
Total	701.333	53			

H4<sub>02</sub> = Inherent factors are not significantly related to the perceived security awareness level of end users of the Gen X generation.

H4<sub>02</sub> considered the relationship between inherent factors and the participants' perceived cyber security awareness levels for the Gen X generational cohort. The questions related to inherent factors were generally an examination of the Gen X participants' personal factors, such as their interest in participating in training, their knowledge level, and the value they placed on cyber security within their organizations.

A scatter plot was used to determine the relationship between the two continuous variables, inherent factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between inherent factors and the level of perceived security awareness of the Gen X participants with number of outliers (Figure 32). Upon establishing the existence of a linear relationship through the scatter plot, the Pearson *r* bivariate correlation coefficient was computed to assess the relationship between inherent factors and the level of perceived security awareness. The Pearson *r* bivariate correlation indicated that there existed a weak correlation between variables with  $r = 0.584$ ,  $n = 52$ , and  $p = 0.000$  (Table 31). The significance value was .000, indicating that a strong significance existed; therefore, the null hypothesis H4<sub>02</sub> could be rejected. Further exploration of the significance of variables was

conducted with an *ANOVA* (Table 32), indicating a significant difference existed as  $p = .007$  ( $p < .050$ ).

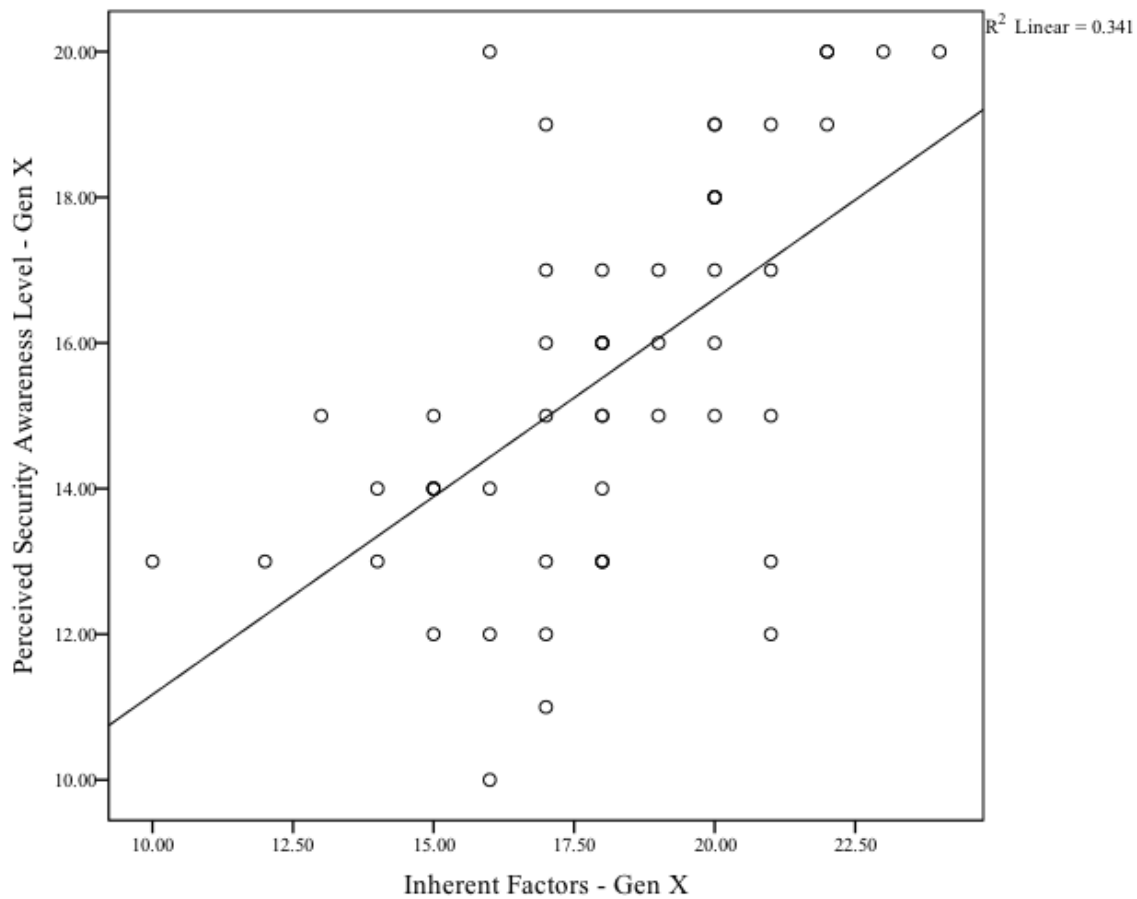


Figure 12: Scatter plot - Inherent Factors (Generation X)

Table 31: Pearson Correlation - Inherent Factors (Generation X)

		PSAL (GX)	IF (GX)
PSAL (GX)	Pearson Correlation	1	.584**
	Sig. (2-tailed)		.000
	N	52	52
IF (GX)	Pearson Correlation	.584**	1
	Sig. (2-tailed)	.000	
	N	52	52

\*\* Correlation is significant at the 0.01 level (2-tailed).

Table 32: *ANOVA* - Inherent Factors (Generation X)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	173.342	10	17.334	2.953	.007
Within Groups	240.658	41	5.870		
Total	414.000	51			

H4<sub>03</sub> = Inherent factors are not significantly related to the perceived security awareness level of end users of the Millennial generation.

H4<sub>03</sub> considered the relationship between inherent factors and the participants' perceived cyber security awareness levels for the Millennial generational cohort. The questions related to inherent factors were generally an examination of the Millennial participants' personal factors, such as their interest in participating in training, their knowledge level, and the value they placed on cyber security within their organizations.

A scatter plot was used to determine the relationship between the two continuous variables, inherent factors, and the level of perceived security awareness. Overall, there was a positive linear relationship between inherent factors and the level of perceived security awareness of the Millennial participants with number of outliers (Figure 33). Upon establishing the existence of a linear relationship through the scatter plot, the Pearson *r* bivariate correlation coefficient was computed to assess the relationship between inherent factors and the level of perceived security awareness. The Pearson *r* bivariate correlation indicated that there existed a strong correlation between variables with  $r = 0.818$ ,  $n = 65$ , and  $p = 0.000$  (Table 33). The significance value was .007, indicating that a strong significance existed; therefore, the null hypothesis H4<sub>03</sub> could be rejected. Further exploration of the significance of variables was

conducted with an *ANOVA* (Table 12), indicating that a significant difference existed as  $p = .000$  ( $p < .050$ ).

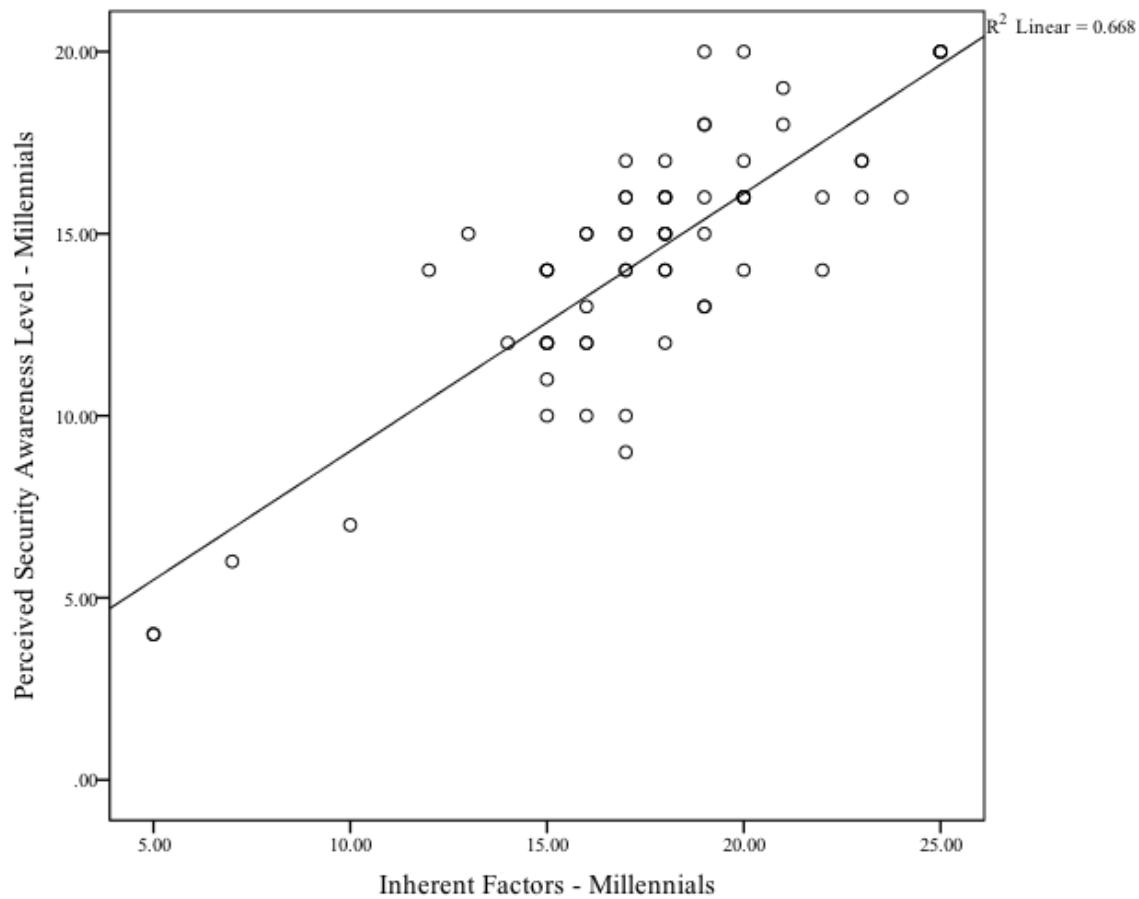


Figure 13: Scatter plot - Inherent Factors (Millennial)

Table 33: Pearson Correlation - Inherent Factors (Millennial)

		PSAL (M)	IF (M)
PSAL (M)	Pearson Correlation	1	.818**
	Sig. (2-tailed)		.000
	<i>N</i>	65	65
IF (M)	Pearson Correlation	.818**	1
	Sig. (2-tailed)	.000	
	<i>N</i>	65	65

\*\* Correlation is significant at the 0.01 level (2-tailed).

Table 34: ANOVA - Inherent Factors (Millennial)

	Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Between Groups	791.399	14	56.529	11.558	.000
Within Groups	244.539	50	4.891		
Total	1035.938	64			

### Summary

This chapter introduced a compilation and presentation of the data collected using a series of statistical analyses. The researcher conducted a collection of demographical data from the three generational cohorts, and descriptive statistics enabled the researcher to portray the quantitative data in a concise and visual manner. Using a histogram and a *QQ* plot, the goodness of fit relative to the normal distribution of the demographical data were visually examined. In the analysis of the responses provided by the respondents, a scatterplot was used to visualize the relationship between variables, followed up by a Pearson correlation that indicated the generational cohort possessing the strongest linear relationship between the independent and dependent variables. Upon determination of the relationship between the two variables, an *ANOVA* was conducted to examine whether there existed a significant statistical difference between the two variables.

## **CHAPTER 5. DISCUSSION, IMPLICATIONS, AND RECOMMENDATIONS**

### **Summary**

Organizations, whether they are small family run businesses, medium-sized companies, or large multinational organizations, place some degree of reliance on IS/IT for the conduct of their business. This dependence is evident when we see the full spectrum of companies operating with a website and an email address; these two components alone are an indication of the dependence businesses have on IS/IT. While governments and large corporations have the greatest reliance on IS/IT and are the most vulnerable, they also possess the necessary resources to protect their data and intellectual property. The element that research frequently indicates as being the weakest link in the cyber security chain is the end user (Straub & Welke, 1998). Increasing the cyber security awareness of end users can be achieved through cyber security training, policy implementation, and awareness programs put in place by organizations in an attempt to mitigate the risk end users pose to the organizations through NMSVs (Guo et al., 2011). This study examined the factors influencing end user security awareness through a generational lens.

### **Research Questions**

The research questions being considered by this study were:

RQ1: What is the relationship between internal IT factors and the cyber security awareness of end users from each generational cohort?

RQ2: What is the relationship between internal management factors and the cyber security awareness of end users from each generational cohort?

RQ3: What is the relationship between external factors and the cyber security awareness of end users from each generational cohort?

RQ4: What is the relationship between inherent factors and the cyber security awareness of end users from each generational cohort?

### **Discussion**

For the first time in history, organizations find themselves in the situation where they have employees from four distinct generational cohorts on the payroll (Cekeda, 2012; Houck, 2011). Each of these generational cohorts possesses distinct habits, ethics, and values. These attributes all contribute to their attitudes toward and behaviors regarding organizational security awareness policies. End users who behave in a careless manner contribute to the NMSVs experienced by an organization. The infractions of these careless end users compromise the security policy and investment in technological efforts put forth by the organization (Chen, Ramamurthy, and Wen, 2012). It is clear that cyber security policies do not guarantee end user compliance. Siponen and Vance (2010) explained that over fifty percent of the violations experienced by organizations can be attributed to NMSVs caused by end users' careless behavior. The consequences of these NMSVs are significant, and their effects are no different than those of illegal activities that are purposely directed at the organization.

The generational habits, ethics, and values that define a generational cohort and their attitude towards organizational security were examined through the four factors outlined by Decker (2008) in his research. His study examined four variables or factors that influence the level of cyber security awareness possessed by end users, specifically internal IT, internal management, external, and inherent factors. This study divided the end users into three generational cohorts, Baby Boomers, Generation X, and Millennials (the Silent Generation was left out because there are very few members of this generation remaining in the workforce), to

determine if there was any significant difference in how each factor influenced the perceived level of security awareness of each cohort.

### **Influencing Factors and their Significance in Business**

The first factor examined for its influence on perceived levels of security awareness was the internal IT factor. Internal IT factors encompass security awareness in the workplace, particularly security awareness training, the use of antiviruses and spam filters, the frequency of mandatory password changes, and acceptable use policies.

The enhancement of internal IT factors in the workplace to minimize instances of NMSVs and increase the level of security awareness will be the responsibility of the executives responsible for the development of policy and IS/IT managers. IS/IT managers in an organization will need to proactively undertake the responsibility of determining the technical aspects of the organization's internal IT factors. Knowing the patterns of threats that exist within their particular organization, IS/IT managers need to determine the type of awareness training that should be implemented within the organization.

In addition to end user training and education, technical aspects need to be examined, and the CIO will need to approve various measures to enhance the internal IT factors. A variety of technical solutions exist that can be established to assist executives and managers in controlling their IT systems. An example will be to include antivirus software and a positive control measure that will ensure regular updates of virus definitions. Spam filters will be beneficial as one of the more common NMSVs occurs when end users, reply to, forward, or click on links embedded in malicious emails.

IS/IT managers and CIO staff must examine the threats that exist and make their recommendations. Governance and policy must then be incorporated to enforce these measures



to ensure greater security of the organizational IS/IT systems. Deviation from the established policy will need to carry swift and severe penalties to minimize the likelihood of occurrence. Enforcement of policy will be the responsibility of executives within the organization.

Based on the results of this study, Baby Boomers and Millennials are equally influenced by internal IT factors, while Generation X is significantly less influenced by internal IT factors. These findings indicate that Boomers and Millennials are already well influenced by this factor and more effort should be concentrated on the Generation X cohort to increase their level of security awareness.

The second factor examined for its influence on the perceived level of security awareness of end users was the internal management factor. Internal management factors include participants' awareness of management's role in the workplace as it relates to security awareness. The questions related to the seriousness that management placed on IT security, whether initial and updated IT security training was included in their workplaces, the discussion of IT security policies, the emphasis on IT security training, and the understanding of the penalties for security violations.

From the name of this factor, it is obvious that responsibility for this factor lies with the managers in the organization. One of the responsibilities of managers is to set a good example for employees and to ensure that their expectations of employees are clear. Effective IT governance will need to be in place to assist managers in the performance of their duties and will clearly delineate what is expected of employees.

The role of the manager is crucial for the internal management factor affecting security awareness, and the greater emphasis management places on demonstrating through their own attitudes the importance of security policies in the workplace and their support of security

awareness training, the greater the positive effect on employees. Organizations must ensure security compliance among all end users, and it is critical that managers at all levels embrace security behavior and display this attitude and belief to all employees.

Based on the results of this study, Baby Boomers are the most influenced by internal management factors, followed closely by Millennials. Generation X is again significantly less influenced by internal management factors. These findings indicate that Boomers and Millennials are already well influenced by this factor and that more effort will need to be concentrated on the Generation X cohort to increase their level of security awareness.

The third factor examined in this study are the external factors that influenced the participants' perceived level of security awareness. External factors involve how government regulations, media reporting, one's educational background in information security, and advisories from financial institutions all affect respondents' perceived security awareness level.

External factors are factors that organizations have no control over. While executives and managers can influence the two previous factors, they will be unable to control external factors. Executives and managers can only use external factors to reinforce their security awareness and posture in the workplace. When breaches in security are compelling stories in the media, management should take the opportunity to enhance their internal management factors by demonstrating the importance of the internal IT factors to end users. The organization can use the example of the external breach to develop their security awareness training within the organization. The implications of the external breach will be more relevant in the minds of employees as management will have previously reinforced it.

Based on the results of this study, Millennials are the most influenced by external factors, followed by Generation X. External factors had significantly less impact on the Baby Boomer

cohort. These findings indicate that Millennials are already well influenced by this factor, and more effort will need to be concentrated mainly on the Baby Boomers, followed by Generation X, to increase their level of security awareness.

The fourth and final factor examined in this study is comprised of the inherent factors that influence participants' perceived level of security awareness. Inherent factors include issues such as respondents' motivation towards information security, their level of interest in attending training to upgrade their computer skills, and their perceived level of computer knowledge.

Unlike external factors, inherent factors are factors that organizations can have a great deal of control over. When end users join an organization, they will bring with them the inherent values from their previous organizations and their own personal inherent values. For the organization to influence the inherent factors found in a new employee, managers will need to ensure early exposure to internal IT and management factors to inculcate the new member with the IS/IT security values of their new organization. These efforts will be more successful if the internal management factors reinforce the internal IT factors that new end users are experiencing.

From the influence of these four factors, it can be seen that all four work symbiotically, and while some have a greater influence over particular generational cohorts than others, it is important for organizations to treat all factors with equal importance as they are symbiotic in nature. It is not possible to achieve a strong level of security awareness in end users if each component or factor examined is treated in isolation. Consideration of all four factors is essential in the formation of IS/IT security policy and IT governance in general. Executives need to ensure that managers have the authority and knowledge necessary to carry out their functions to ensure adequate cyber security. The harmonious blending of these four factors will achieve

the greatest results and see a reduction in the number of NMSVs and an increase in overall security awareness within the multigenerational workforce.

### **Primary Motivating Factors by Generational Cohort**

These three generations inhabit a unique place in history and the future due to the new relevance of IT/IS in their lives. The Baby Boomers, for the most part, were not influenced by computers in their youth, as they were unlikely to encounter computers until they were at least of college age. Generation X was significantly affected by the introduction of computers into everyday life. The oldest Generation Xers saw the Apple II, IBM 8088 and 8086, Tandy, and Commodore 64 computers enter the market and programming start to become a part of high school curricula. The younger Gen Xers saw more advanced computers possessing Intel Pentium technology enter the market. They also experienced the beginning of an online community through local Bulletin Board Services (BBS). In the early 1990s, the Internet became available through local Internet service providers (ISPs) and accessible through browsers such as Netscape, something that had initially only operated on Unix systems in universities. It did not take long before Gen Xers became fully engaged in the World Wide Web through their IBM-compatible personal computers and their dial-up modems. Most of the Millennial generation has grown up in an environment where a computer has always existed in the home, or at least they have had easy access to one through school or public libraries. This generation has never known the world without IS/IT. Given the significant and distinct differences in perception these three generations have regarding computers and IS/IT, it is important to examine the three generational cohorts separately to observe the differences in their perceived security awareness and how the four different factors influence each cohort.

## **Baby Boomer**

The data were examined using the Pearson correlation to determine the factors affecting the perceived security awareness level of the Baby Boomer cohort. The factors, in order of priority, are as follow:

1. Internal Management ( $r = .702$ ),
2. Internal IT ( $r = .645$ ),
3. Inherent ( $r = .613$ ), and
4. External ( $r = .588$ ).

From these results, we see that internal management factors are the primary motivating factors influencing security awareness in the Baby Boomer cohort. This result is expected, as this generational cohort is known for its propensity to possess a strong devotion to work and its desire to develop and follow rules (Cekada, 2012). According to Gelston (2008), the Baby Boomer cohort is seen as the annoying cohort by the Generation X and Millennial cohorts due to their apparent workaholic attitude. Gelston goes on to say that 68 percent of Baby Boomers feel that Gen Xers and Millennials do not possess the proper work ethic. When examining the ethical beliefs and work habits of the Baby Boomer generation, it can be seen that they tend to become workaholics who are willing to make sacrifices for their career. This generational cohort also firmly believes that employees must “pay their dues” to the organization before they are allowed to reap any rewards. This attitude is significantly different than that of the other two cohorts studied, who believe this is not a necessary component of the workplace. Internal factors, both management and IT, are the greatest influence on the Baby Boomer generation. This cohort was expected to begin retiring en masse around 2008 or 2009; however, given the economic downturn that started in 2007, the Baby Boomers have remained in the workplace. This cohort

continues to occupy leadership positions, much to the displeasure of Gen Xers and Millennials who believe the Baby Boomers should leave as they have been in these positions for too long.

## **Generation X**

The data were examined using the Pearson correlation to determine the factors affecting the perceived security awareness level of the Generation X cohort. The factors, in order of priority, are as follows:

1. External ( $r = .605$ ),
2. Internal Management ( $r = .592$ ),
3. Inherent ( $r = .584$ ), and
4. Internal IT ( $r = .532$ ).

From these results, we see that external factors are the primary motivating factors influencing security awareness in the Generation X cohort. This finding falls in line with what we know of Generation X. The other two cohorts view Generation X as being lazy, skeptical, and cynical. Baby Boomers and Millennials both view Generation X negatively, a view this generation does not accept as they feel they are practical, observant, and adaptable due to the challenges they had growing up. Simons (2010) supports the finding that external factors are the most influential on Generation X as he states they have a tendency to reject rules, enjoy living life on the edge, and possess an innate distrust of institutions. Cekada (2012) claimed that Gen Xers have no loyalty to organizations because of the observations they made as youngsters when their parents faced insecurity and layoffs. Generation X was the first generation to see mass layoffs affecting their families due to the recession in the early 1980s, causing them to become indifferent to organizations, contrary to their parents from the Baby Boomer generation. This fact solidifies the researcher's finding that internal factors did not play as significant a role as

external factors. This generation does not possess the same loyalty to their employers as the previous generations.

## **Millennials**

The data were examined using the Pearson correlation to determine the factors affecting the perceived security awareness level of the Millennial cohort. The factors, in order of priority, are as follow:

1. Inherent ( $r = .818$ ),
2. Internal IT ( $r = .664$ ),
3. Internal Management ( $r = .660$ ), and
4. External ( $r = .625$ ).

From these results, we see that inherent factors are the primary motivating factors influencing security awareness in the Millennial cohort. From the review of the literature, the Millennial generation is most influenced by inherent factors as it is the “me” generation and a generation that can quickly assimilate technology. However, it possesses the same lack of loyalty to organizations as Generation X. This cohort grew up having to rely on their own abilities as they grew up in a recession in which finding employment proved difficult.

Additionally, the Millennials were given much attention when they were youngsters, resulting in unfounded self-confidence as they grew up in a “child-centric” era. This generational cohort is described as the entitled generation, possessing a confidence that can be mistaken for arrogance. Verschoor (2013) supports the finding that inherent factors play the most significant role by explaining that Millennials are not loyal to organizations and that they demand immediate feedback and recognition. Wilson (2009) also supports the finding that inherent factors are the most significant factor as he describes Millennials as needy, indulged, entitled, and self-

absorbed. From the results of this research and the research of other scholars, it is apparent that inherent factors are the primary motivating factor for the Millennial generation.

### **Recommendations**

Decker's (2008) research on the factors affecting the security awareness of end users contributed to the body of knowledge regarding end users and their security awareness level. Holbert's (2013) research augmented Decker's research by examining which of the four factors had the greatest influence on security awareness. Using the Decker survey tool, this research builds upon the prior research of these two scholars.

The intent of this study is to increase the body of knowledge regarding best practices and practical security awareness training methodologies that can influence positive change in a multigenerational workforce. By identifying which of the four factors resonates best with each generational cohort, it will be possible for organizations to develop targeted cyber security policies and awareness training that best relates to the generational cohorts within their organization.

It is clear from this study that the three generational cohorts are influenced to different degrees by each of the factors affecting security awareness. This does not indicate that organizations should concentrate their efforts exclusively on the single factor that most affects security awareness. Organizations need to treat the four factors holistically; the four factors rely on each other to ensure a greater degree of security awareness. External and inherent factors are not factors the organization can initially control. External factors can be made examples of to reinforce internal IT factors, and inherent factors can be influenced then enhanced by both internal IT and management factors.



Large organizations typically conduct their cyber security awareness training online using computer-based training programs. The employees' generations are not taken into consideration in these training programs. The training usually consists of a "one size fits all" method of training. From the employee metadata found in their login profiles, the generational cohorts of end users can easily be determined. Their generational cohorts could then influence subsequent training, training that has been developed and structured to accommodate a variety of factors including their generational cohort. As demonstrated in this study, each cohort responds differently to each of the four factors. Organizations can target specific training for different end users depending on their generational cohort. This will ultimately ensure that greater security awareness is achieved through targeted training. Adjusting security awareness policies and training according to the end users' generational cohort is a method organizations can use to decrease their number of NMSVs.

Educators have examined the influence different generational cohorts have on education and how these differences should be considered in instructional design, and researchers have studied the training methodologies best suited to particular generations (Cekada, 2012; Farrell & Hurt, 2014; Reeves & Oh, 2008). In a study conducted for IBM, Lesser and Rivera (2006) discovered that differences occur and that there exists a need to diversify the methodology and content of the training being offered to be beneficial throughout the multigenerational workplace.

Each generational cohort responds differently to different teaching styles. Hence, by understanding which methods work best for the different generations, instructional designers will be better prepared to design effective training plans. When developing security awareness training, educators should take into consideration the primary motivational factors in each

generational cohort. Training should then be tailored to each student according to the generational cohort to which he or she belongs. As a result, end users will be better trained and better able to positively affect the level of security in the IT/IS in their organizations.

### **Further Research**

A limitation of this study was that it was not conducted in a homogeneous environment. It would be beneficial to conduct further studies regarding the factors affecting security awareness in large corporations that possess employees from all three generational cohorts. By doing this, the respondents would theoretically all have had the same level of institutional cyber security training. The responses would then be more directly related and the generational differences would be more pronounced. Additional research could then be conducted on each generation and on the one factor that had the greatest influence on that cohort's level of security awareness. This would allow organizations to further refine their awareness training and policy development to best suit their needs, ultimately reducing the risk posed by end users through NMSVs.

Within this homogeneous environment, the research could explore the roles of the variables of age, experience, and longevity in the workplace and their correlation with cyber security awareness. As members of each generational cohort grow older, it is possible that their experience in the workplace and their age will play a role in their level of security awareness and will be more influential than their generational cohort. Another factor that could be examined would be what degree of influence an increased level of responsibility has on end users' level of security awareness. As employees progress in responsibility and take on greater managerial roles, would this increased level of responsibility have a greater influence on their level of security awareness than their generational cohort? This would likely have a greater influence on

their level of security awareness, as they would then be responsible for the policies and the implementation of security awareness training.

Further research could also be conducted into the way future generational cohorts will be defined, and on the impact of this on cyber security awareness. McCrindle and Wolfinger (2010) stated that the traditional, biologically based definition of a generation as being a 20 – 25 year span is no longer applicable as the generational cohorts are changing faster than in previous generations, and that a proper definition is primarily influenced by technological advances and the significant changing of societal values (McCrindle & Wolfinger, 2010). As such, the authors claimed that two decades is far too long when considering a generation. An examination could be conducted to explore what will define future generations if generational cohorts are no longer biologically driven. Given the rapid pace at which technology is evolving, it is possible that generational cohorts will become shorter in the future. An examination of these potentially shorter cohorts may reveal potential problems in cyber security awareness in the future.

## References

- Al-Asfour, A., & Lettau, L. (2014). Strategies for leadership styles for multi-generational workforce. *Journal of Leadership, Accountability & Ethics, 11*(2), 58-69.
- Anderson, D., Sweeney, D., & Williams, T. (2014). *Essentials of modern business statistics with Microsoft Excel* (5th ed.). Stamford, CT: Cengage Learning.
- Bell, E. E. (2008). *Multigenerational workplace performance: Generational similarities and differences in employee perception of the work environment.*, Capella University, Ann Arbor. ProQuest Dissertations & Theses Global database. (No. 3296639)
- Beyers, R. N. (2009). A five dimensional model for educating the net generation. *Educational Technology & Society, 12*(4), 218-227.
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.  
doi:<http://dx.doi.org/10.1057/ejis.2009.8>
- Cekada, T. L. (2012). Training a multigenerational workforce. *Professional Safety, 57*(3), 40-44.
- Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157-188.
- Cooper, D. R. (2011). *Business Research Methods*, (11<sup>th</sup> ed.). New York, NY: McGraw-Hill/Irwin
- Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.

- Davis, J. B., Pawlowski, S. D., & Houston, A. (2006). Work commitments of baby boomers and Gen-Xers in the IT profession: Generational differences or myth? *Journal of Computer Information Systems*, 46(3), 43-49.
- Decker, L. G. (2008). *Factors affecting the security awareness of end-users: A survey analysis within institutions of higher learning.*, Capella University, Ann Arbor. ProQuest Dissertations & Theses Global database. (No. 3290951)
- Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, 45(1), 67-87.
- Farrell, L., & Hurt, A. C. (2014). Training the millennial generation: Implications for organizational climate. *E Journal of Organizational Learning & Leadership*, 12(1), 47-60.
- Fehr, E., & Schmidt, K. M. (2007). Adding a stick to the carrot? The interaction of bonuses and fines. *American Economic Review*, 97(2), 177-181.
- Gelston, S. (2008). Welcome to the generation wars. *CIO*, 21(8), 38-40.
- Gilburg, D. (2008). They're Gen Y and you're not. *CIO*, 21(8), 40-43.
- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2), 203-236.
- Harris, M. A. (2010). *The shaping of managers' security objectives through information security awareness training.*, Virginia Commonwealth University, Ann Arbor. ProQuest Dissertations & Theses Global database. (No. 3413852)
- Hicks, M., & Block, L. (2014). "What's in it for me?" Targeting rewards messaging to all generations. *Benefits Quarterly*, 30(2), 47-50.

- Holbert, D. A. (2013). *Factors contributing to security awareness of the end user.*, Capella University, Ann Arbor. ProQuest Dissertations & Theses Global database. (No. 3605034)
- Houck, C. (2011). Multigenerational and virtual: How do we build a mentoring program for today's workforce? *Performance Improvement*, 50(2), 25-30. doi:10.1002/pfi.20197
- Howe, N., & Strauss, W. (1991). *Generations: The history of America's future, 1584 to 2069*: New York, NY: Harper Perennial.
- Howe, N., & Strauss, W. (2000). *Millennials rising: The next great generation*. New York, NY: Vintage.
- Howe, N., & Strauss, W. (2007). The next 20 years: How customer and workforce attitudes will evolve. *Harvard Business Review*, 85(7/8), 41-52.
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615-660. doi:10.1111/j.1540-5915.2012.00361.x
- Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management*, 22(2), 7-19.
- Kilber, J., Barclay, A., & Ohmer, D. (2014). Seven tips for managing Generation Y. *Journal of Management Policy & Practice*, 15(4), 80-91.
- Lesser, E., & Rivera, R. (2006). Closing the generational divide: Shifting workforce demographics and the learning function. *International Business Machines (IBM) & American Society of Training and Development (ASTD)*. Somers: NY, IBM.
- Lim, V. K. G., Teo, T. S. H., & Loo, G. L. (2002). How do I loaf here? Let me count the ways. *Communications of the ACM*, 45(1), 66-70.

- Lippincott, J. K. (2010). Information commons: Meeting millennials' needs. *Journal of Library Administration*, 50(1), 27-37. doi:10.1080/01930820903422156
- Ludwick, P. (2007). The boomers are already gone. *Journal of Housing & Community Development*, 64(1), 22-26.
- Mannheim, K. (1952). The sociological problem of generations. *Essays on the Sociology of Knowledge*, 276-322.
- McCrindle, M., & Wolfinger, E. (2010). Generations defined. *Ethos*, 18(1), 8-13.
- McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, 9(1), 23-41.  
doi:10.1080/15332861.2010.487415
- Mohamad Rashid, R., Zakaria, O., & Nabil Zulhemay, M. (2013). The relationship of information security knowledge (ISK) and human factors: Challenges and solution. *Journal of Theoretical & Applied Information Technology*, 57(1), 67-75.
- Prensky, M. (2001). Digital natives, digital immigrants, Part II: Do they really think differently? *On the Horizon*, 9(6), 1-9.
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 767-A764.
- Pullen, J. P. (2013). Smooth criminals. *Entrepreneur*, 41(2), 50-53.
- Reeves, T. C., & Oh, E. J. (2008). Do generational differences matter in instructional design. *Accessed on*, 12(10), 10.
- Simoneaux, S., & Stroud, C. (2010). Bridging the generation gaps in the retirement services workplace. *Journal of Pension Benefits: Issues in Administration*, 17(2), 66-75.

- Simons, N. (2010). Leveraging generational work styles to meet business objectives. *Information Management & Computer Security*(15352897(44)).
- Siponen, M., Mahmood, M. A., & Pahlila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, 52(12), 145-147.
- Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-A412.
- Smola, K. W., & Sutton, C. D. (2002). Generational differences: Revisiting generational work values for the new millennium. *Journal of Organizational Behavior*, 23(4), 363-382.  
doi:10.1002/job.147
- Stokes, P. (2011). *Key concepts in business and management research methods*: Palgrave Macmillan.
- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4), 441-469.
- Straub, J. D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 14(1), 45-60.
- Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276.
- Thielfoldt, D. (2014). Rewire your baby boomers. *The Electrical Distributor*.
- Verschoor, C. C. (2013). Ethical behavior differs among generations. *Strategic Finance*, 95(8), 11-14.
- Von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, 20(3), 215-218.



- Von Solms, B. (2015). The cyber security buck stops right at the top. *Finweek*, 36-37.
- Wilson, L. (2009). Generations at work: The problems, power, and promise explored. *Journal: American Water Works Association*, 101(5), 46-54.
- Wylder, J. O. (2003). Improving security from the ground up. *Information Systems Security*, 11(6), 29.

## APPENDIX A – Statistical Tests

### Reliability Statistics

#### Chronbach's Alpha

Table A1: Chronbach's Alpha – Internal IT Factors

Internal IT Factors	
Cronbach's Alpha	<i>N</i> of Items
.874	5

Table A2: Chronbach's Alpha – Internal Management Factors

Internal Management Factors	
Cronbach's Alpha	<i>N</i> of Items
.849	6

Table A3: Chronbach's Alpha – External Factors

External Factors	
Cronbach's Alpha	<i>N</i> of Items
.643	5

Table A4: Chronbach's Alpha – Inherent Factors

Inherent Factors	
Cronbach's Alpha	<i>N</i> of Items
.682	5

Table A5: Chronbach's Alpha – Perceived Security Awareness Level

Perceived Security Awareness Level	
Cronbach's Alpha	<i>N</i> of Items
.767	4

## Descriptive Statistics

### Internal IT Factors

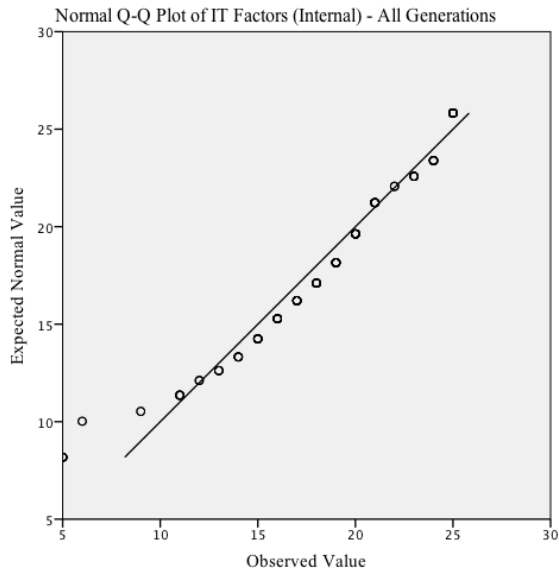


Figure A1: *QQ* Plot - Internal IT Factors (All Generations)

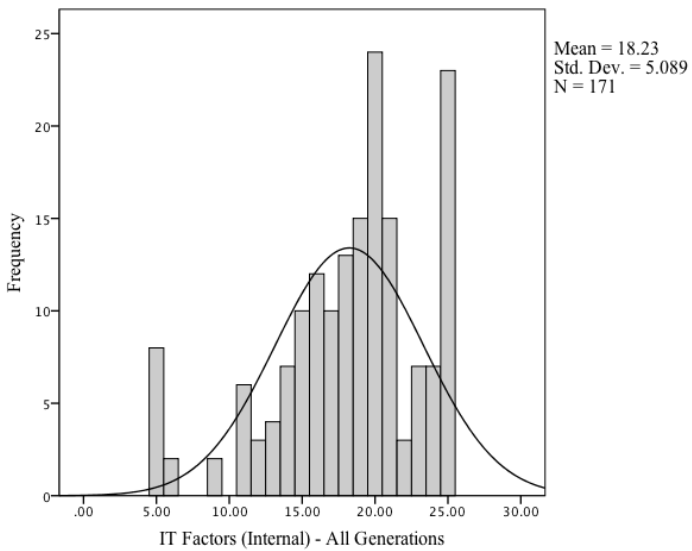


Figure A2: Histogram - Internal IT Factors (All Generations)

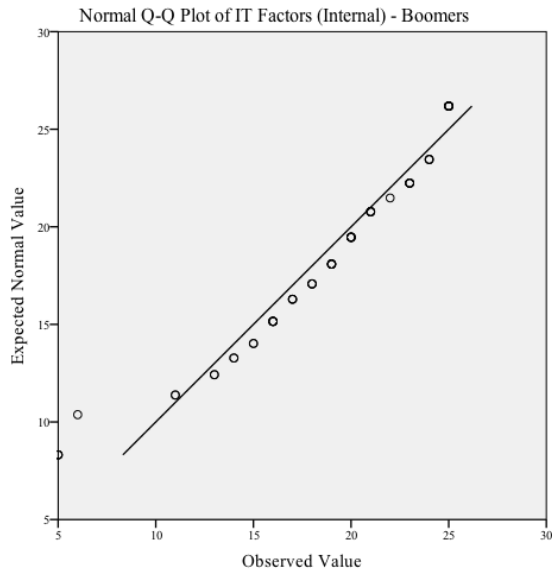


Figure A3: *QQ* Plot - Internal IT Factors (Baby Boomers)

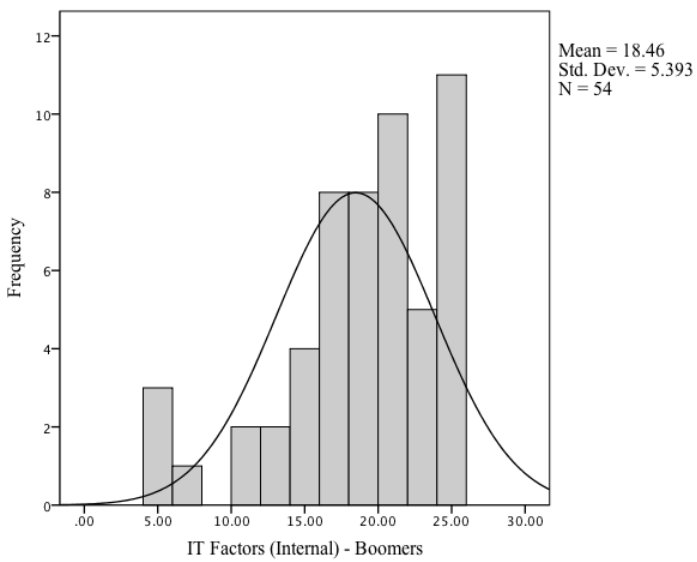


Figure A4: Histogram - Internal IT Factors (Baby Boomers)

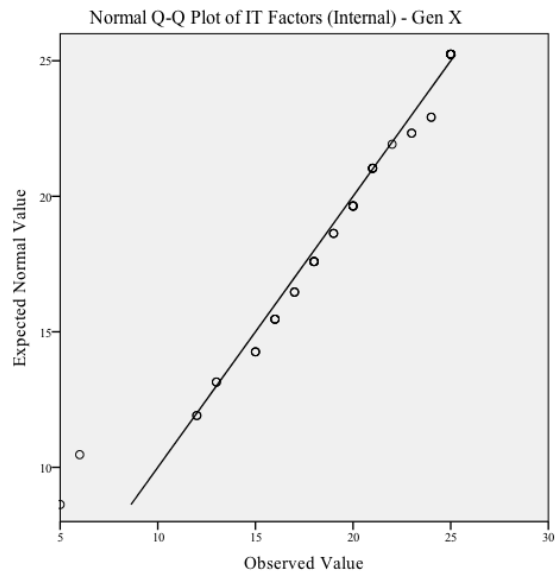


Figure A5: *QQ* Plot - Internal IT Factors (Generation X)

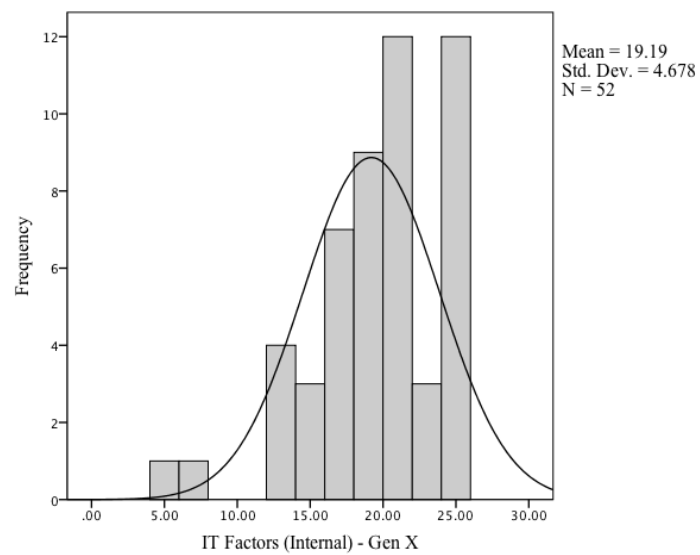


Figure A6: Histogram - Internal IT Factors (Generation X)

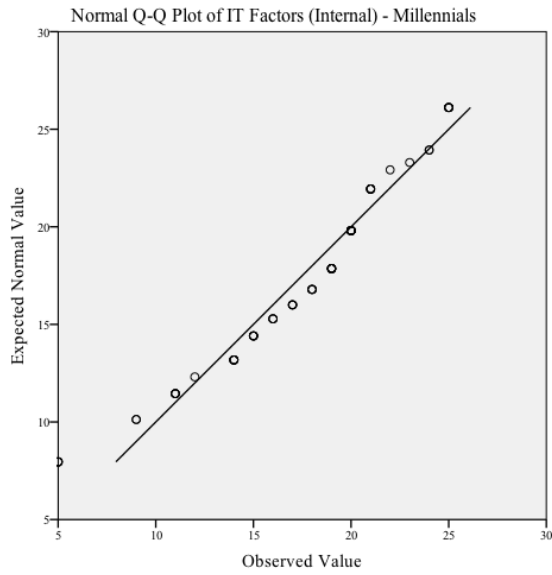


Figure A7: *QQ* Plot - Internal IT Factors (Millennials)

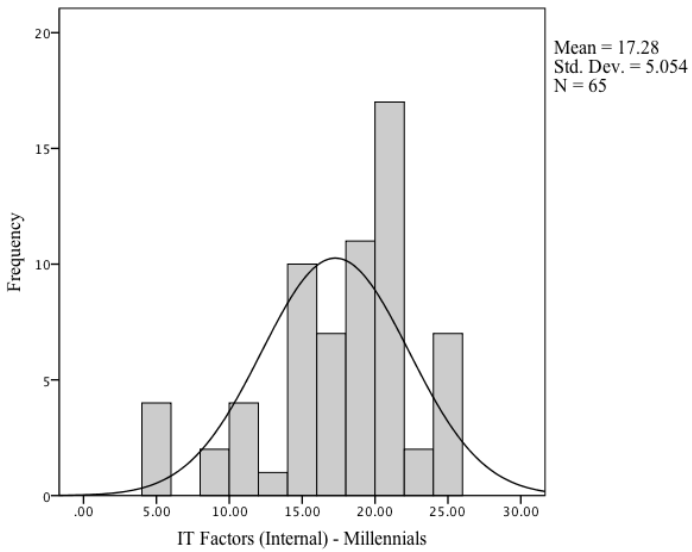


Figure A8: Histogram - Internal IT Factors (Millennials)

## Internal Management Factors

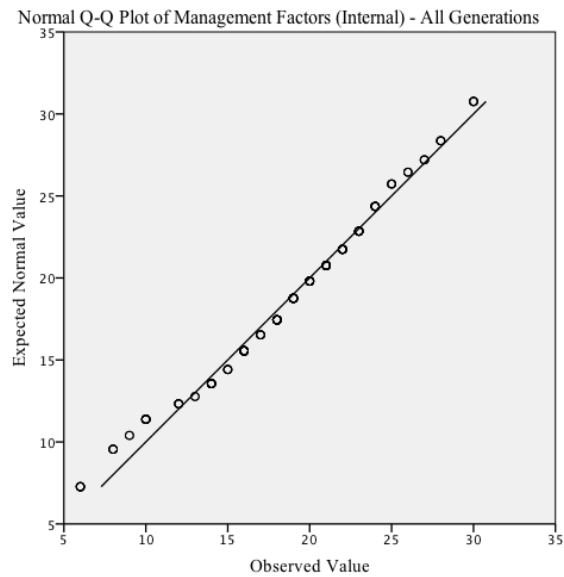


Figure A9: *QQ* Plot - Internal Management Factors (All Generations)

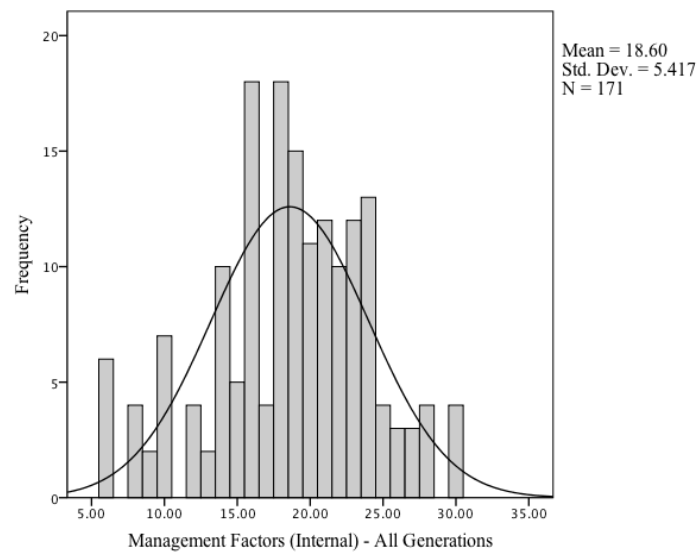


Figure A10: Histogram - Internal Management Factors (All Generations)

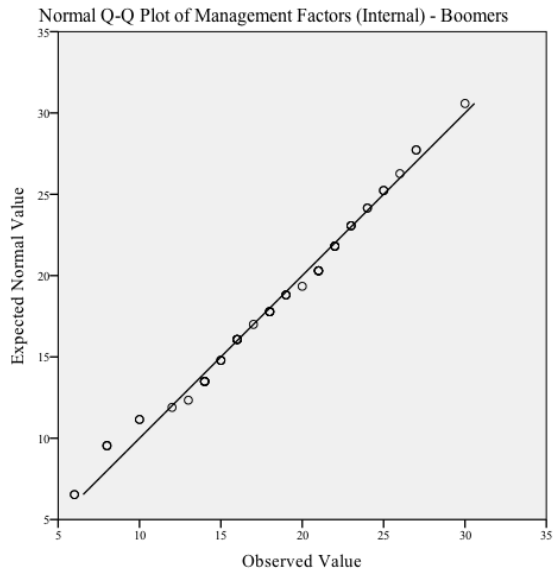


Figure A11: *QQ* Plot - Internal Management Factors (Baby Boomers)

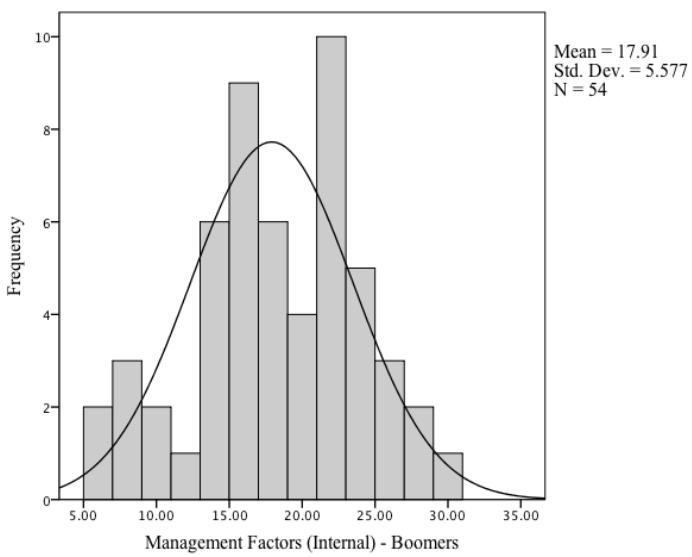


Figure A12: Histogram - Internal Management Factors (Baby Boomers)



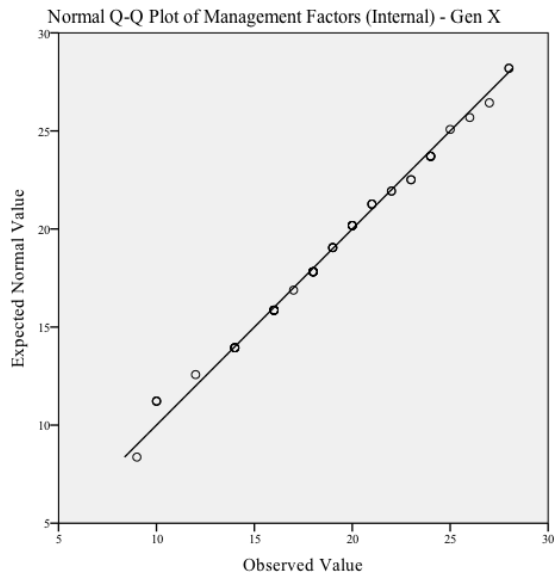


Figure A13: *QQ* Plot - Internal Management (Generation X)

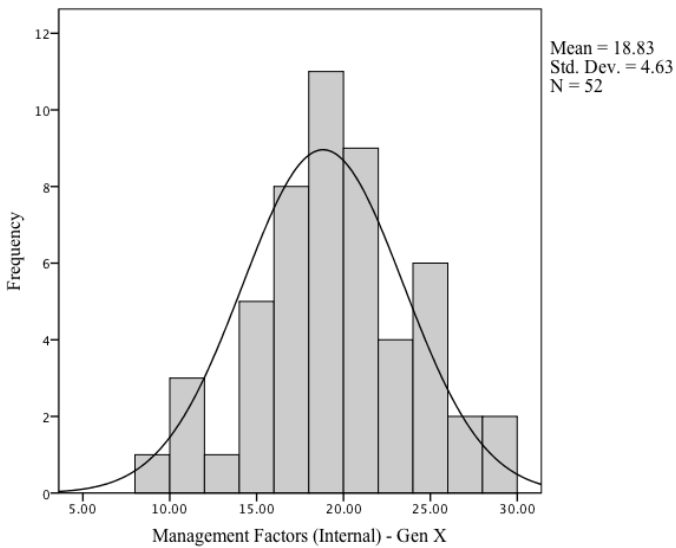


Figure A14: Histogram - Internal Management Factors (Generation X)

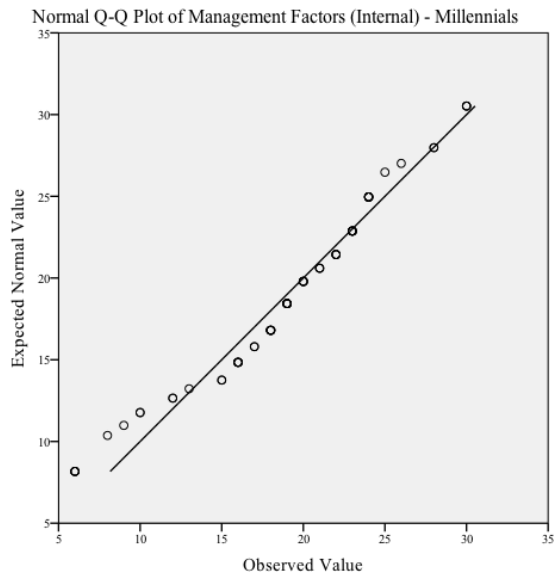


Figure A15: *QQ* Plot - Internal Management (Millennials)

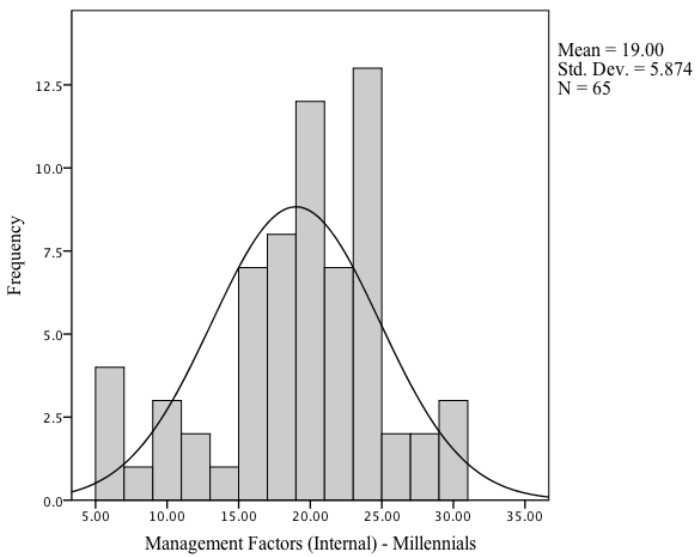


Figure A16: Histogram - Internal Management Factors (Millennials)

## External Factors

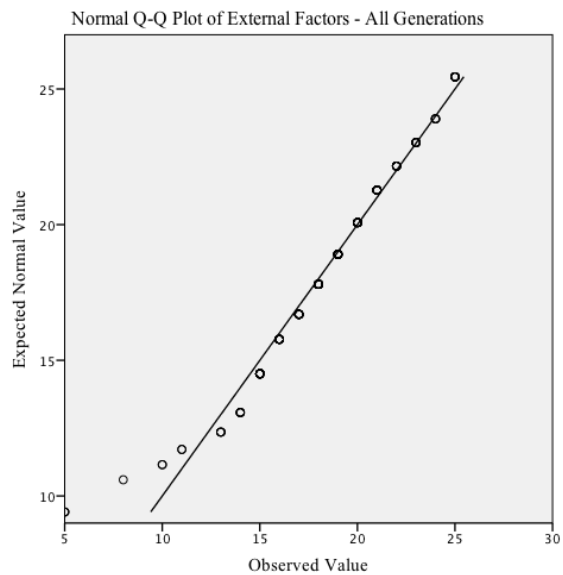


Figure A17: *QQ* Plot - External Factors (All Generations)

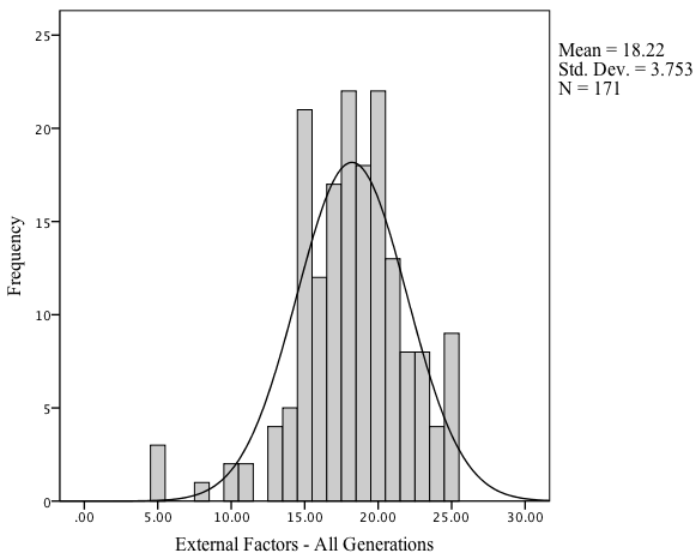


Figure A18: Histogram - External Factors (All Generations)

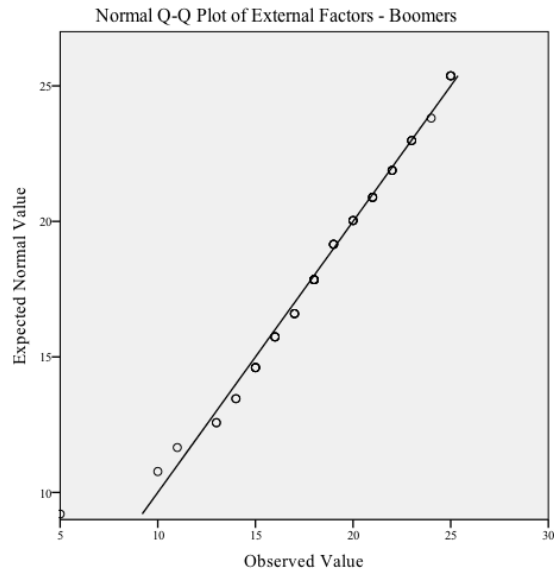


Figure A19: *QQ* Plot - External Factors (Baby Boomers)

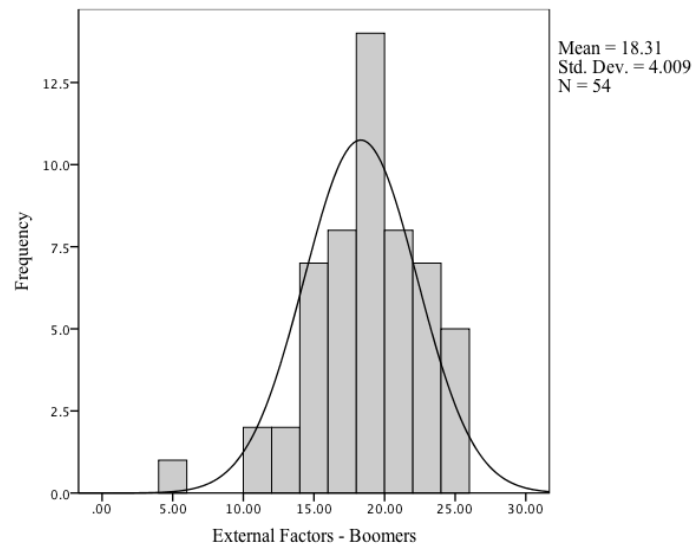


Figure A20: Histogram - External Factors (Baby Boomers)

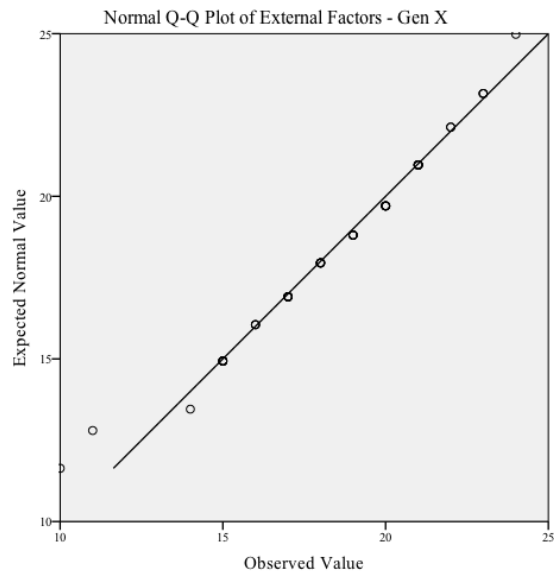


Figure A21: *QQ* Plot - External Factors (Generation X)

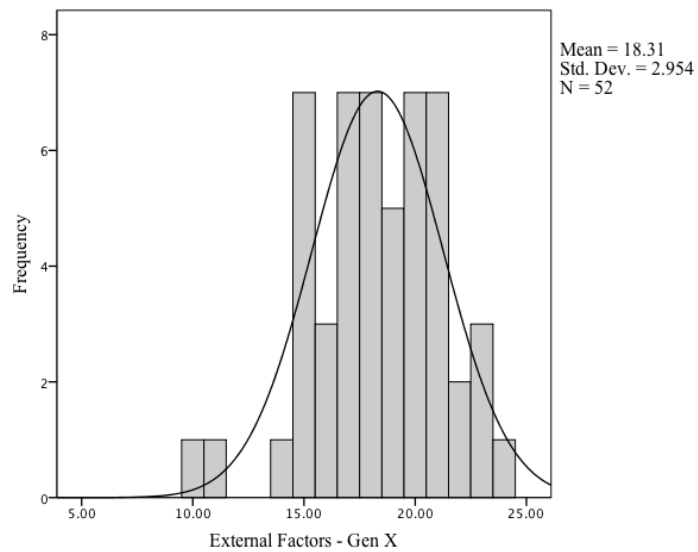


Figure A22: Histogram - External Factors (Generation X)

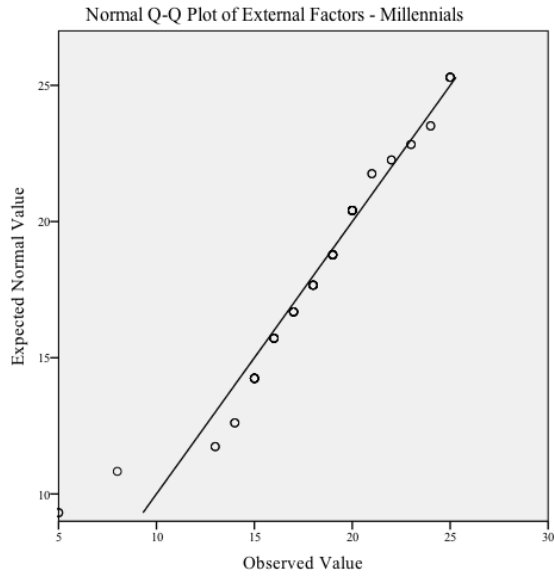


Figure A23: *QQ* Plot - External Factors (Millennials)

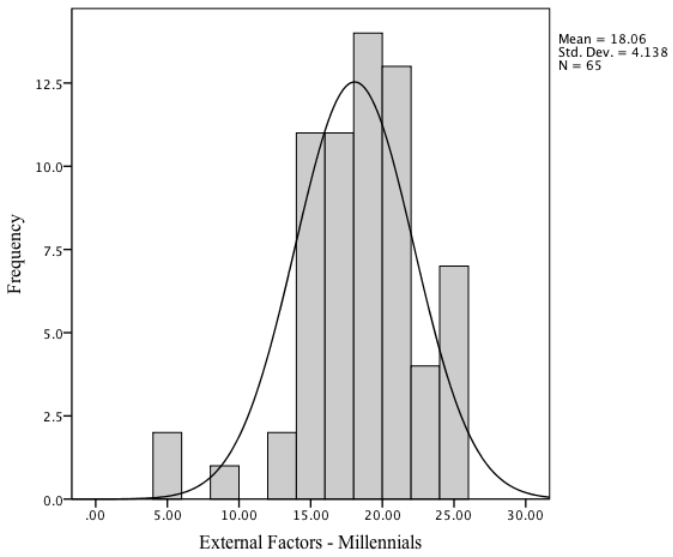


Figure A24: Histogram - External Factors (Millennials)

## Inherent Factors

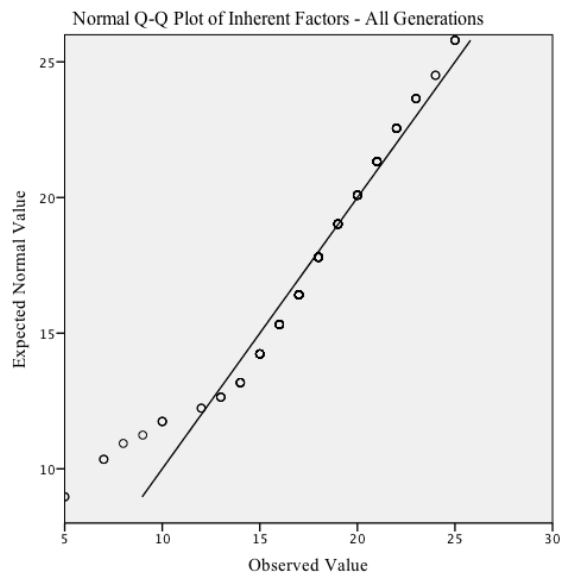


Figure A25: *QQ* Plot - Inherent Factors (All Generations)

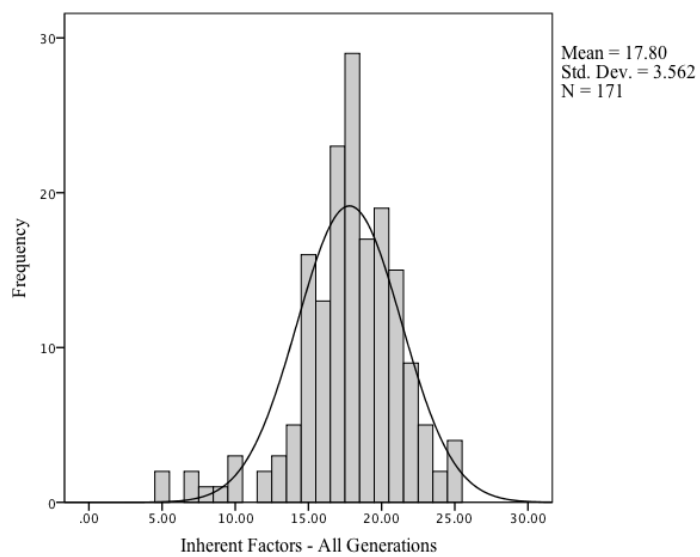


Figure A26: Histogram - Inherent Factors (All Generations)

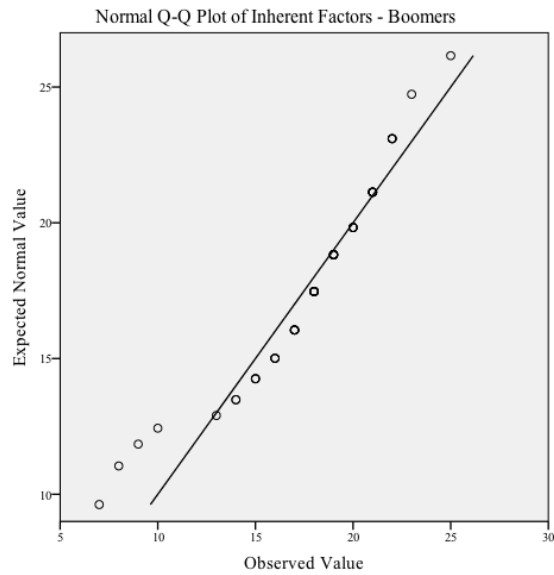


Figure A27: *QQ* Plot - Inherent Factors (Baby Boomers)

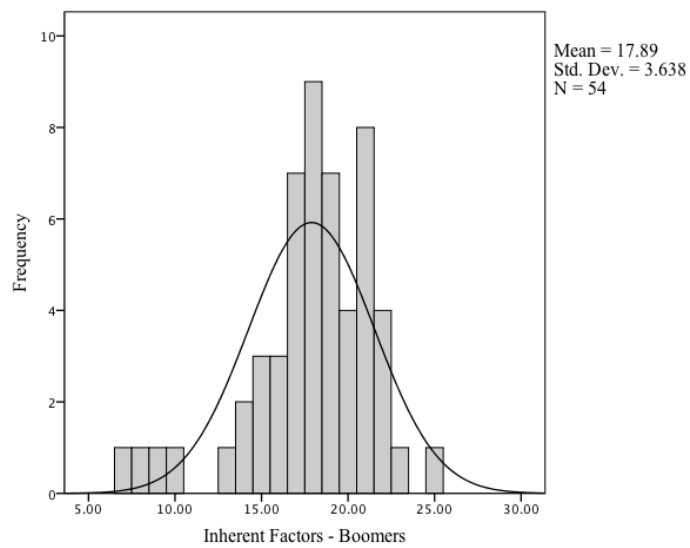


Figure A28: Histogram - Inherent Factors (Baby Boomers)



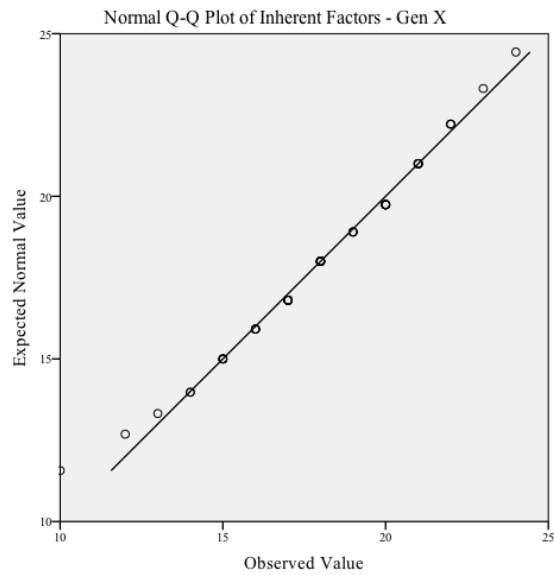


Figure A29: *QQ* Plot - Inherent Factors (Generation X)

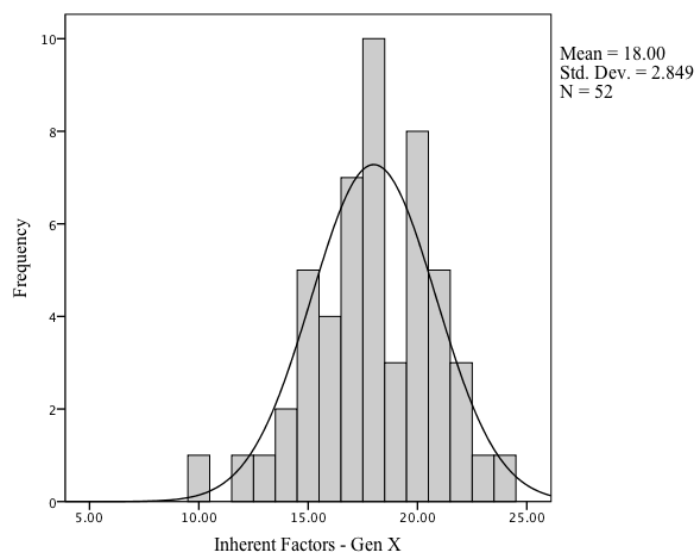


Figure A30: Histogram - Inherent Factors (Generation X)

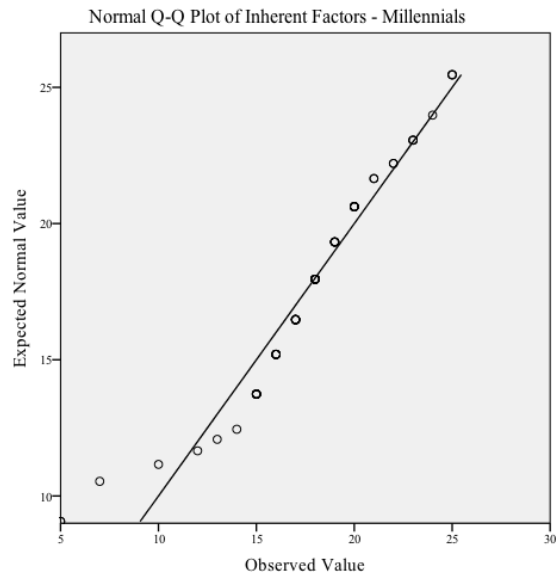


Figure A31: *QQ* Plot - Inherent Factors (Millennials)

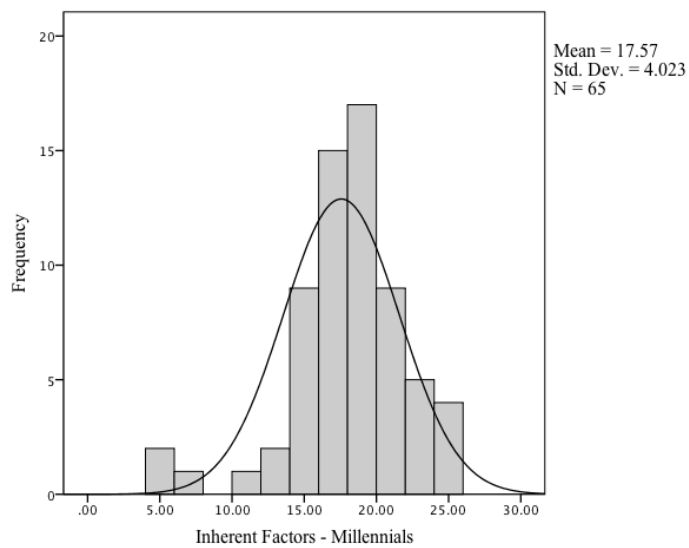


Figure A32: Histogram - Inherent Factors (Millennials)

## Perceived Security Awareness Level

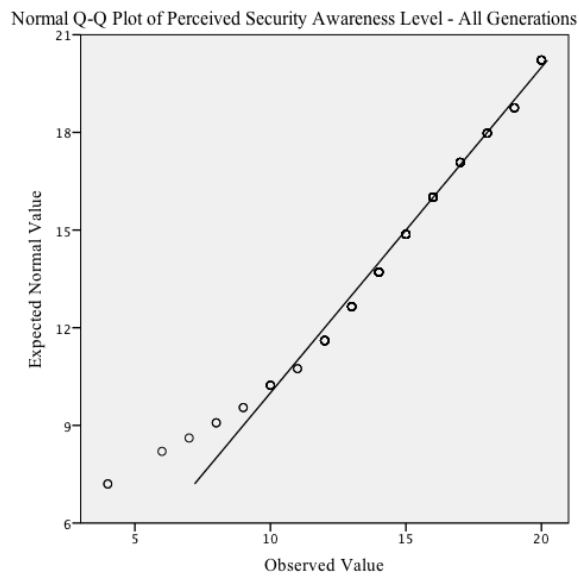


Figure A33: *QQ* Plot – Perceived Security Awareness Level (All Generations)

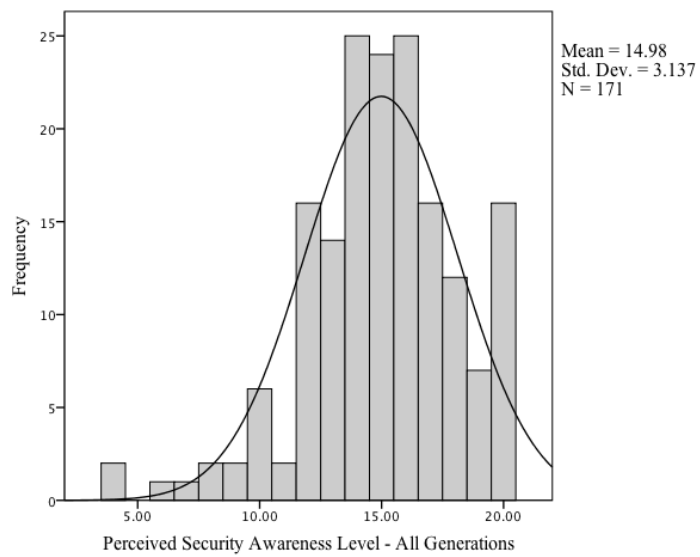


Figure A34: Histogram - Perceived Security Awareness Level (All Generations)

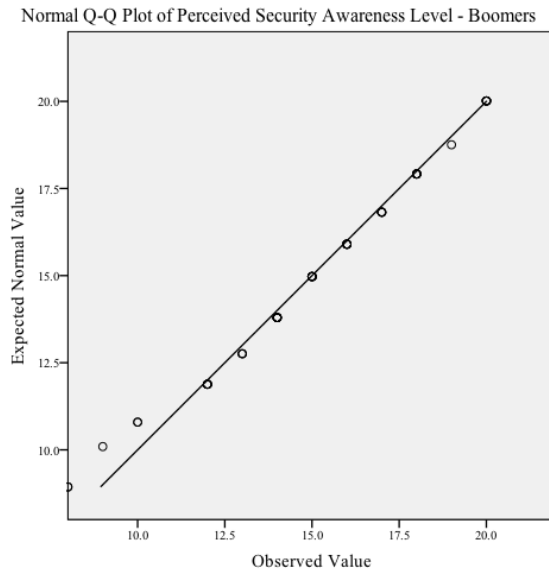


Figure A35: *QQ* Plot - Perceived Security Awareness Level (Baby Boomers)

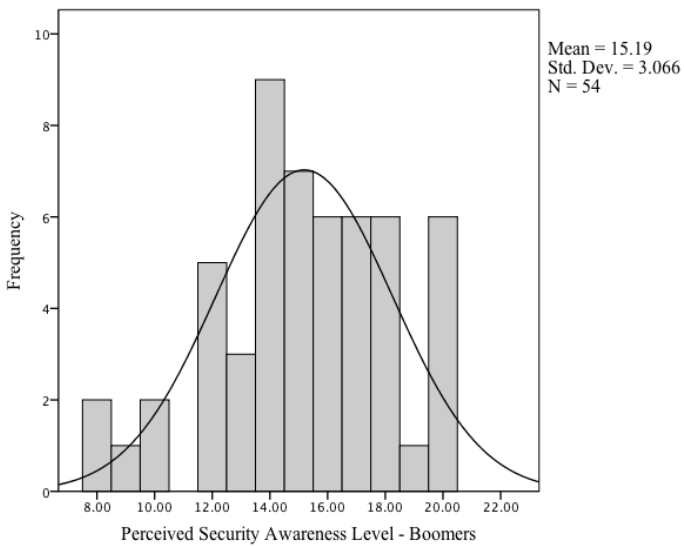


Figure A36: Histogram - Perceived Security Awareness Level (Baby Boomers)

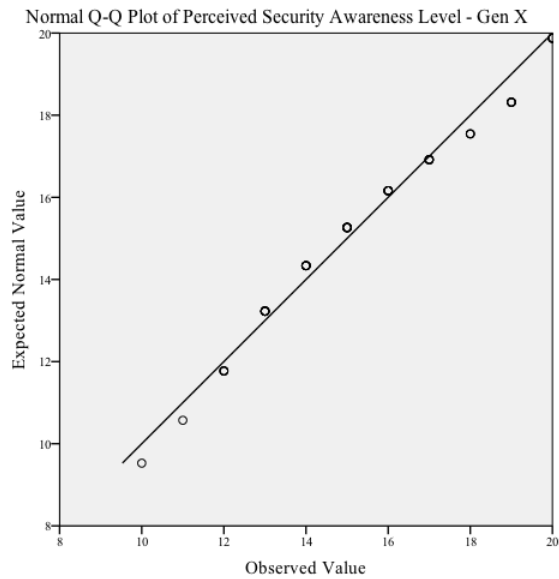


Figure A37: *QQ* Plot - Perceived Security Awareness Level (Generation X)

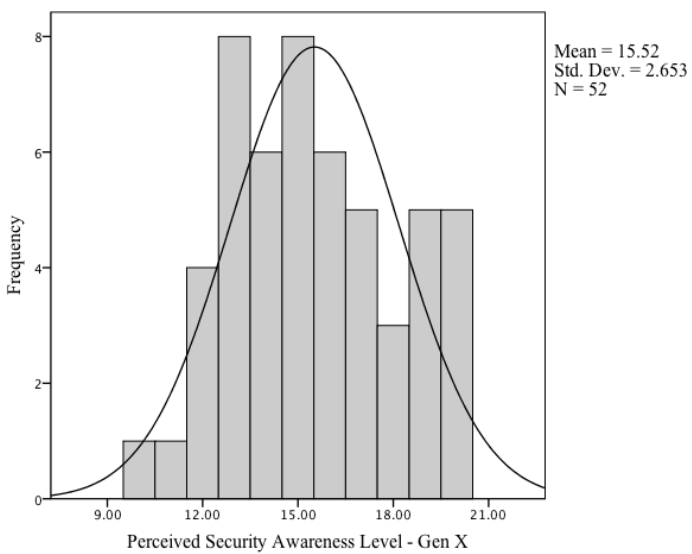


Figure A38: Histogram - Perceived Security Awareness Level (Generation X)

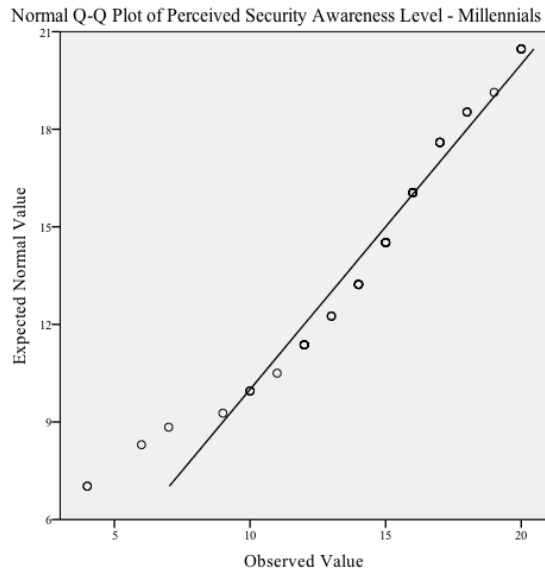


Figure A39: *QQ* Plot - Perceived Security Awareness Level (Millennials)

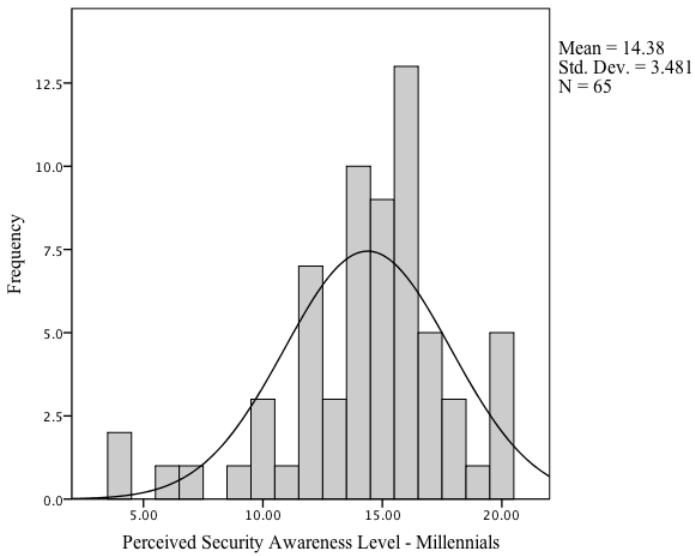


Figure A40: Histogram - Perceived Security Awareness Level (Millennials)

## **APPENDIX B – Survey Instrument**

### Demographic Section:

Please choose one of the following answers:

Which Generational Cohort do you belong to?

1. 1946-1964
2. 1965-1980
3. 1981-2000

What is your gender?

1. Female
2. Male

Employment or Student Status

1. Employed Fulltime or business owner
2. Employed Part time
3. Full time student
4. Part time student
5. Retired
6. Disabled

How long have you been employed at your organization?

1. Under one year
2. One to three years
3. Three to five years
4. Over 5 years to 15 years
5. Over 15 years to 25 years
6. Over 25 years

What is your highest level of education?

1. Less than High School
2. High School or Equivalent (GED)
3. Some College, no degree
4. Associate Degree
5. Bachelor Degree
6. Graduate Degree

Percentage of day on computer

1. 0
2. 1-25
3. 26-50
4. 51-75
5. 75-100

The remaining questions will be based on a Likert Rating Scale of 1 (strongly disagree) to 5 (strongly agree).

#### Section 1: Internal IT Factors (Training)

1. As part of my job I have completed company security awareness training.
2. My organization actively uses antivirus software to increase information security.
3. My organization actively uses Spam filters to increase information security.
4. I am familiar with my organization's Acceptable Use Policy.
5. My organization requires complex passwords that must be changed frequently.

#### Section 2: Internal Management Factors

6. Management within my organization is very serious about information security.
7. Information security training is included as a part of orientation for new employees.
8. Information security policies are discussed during my annual evaluation.
9. Employees in my organization receive updated information or training regarding information security.
10. Attending security training can lead to promotion of higher pay.
11. I understand the penalties for breaches of security in my organization.

#### Section 3: External Factors

12. Following federal and state requirements is an important part of my organization's information security policy.
13. I received information security training as part of my education.
14. I use anti-virus software on my home computer and update it frequently.
15. I have read/seen articles in the news media about information security (e.g. security breach of loss of private information) in the last 30 days.
16. My financial institution frequently sends me information regarding information security (e.g. protection against identity theft).



#### Section 4: Inherent Factors

- 17. I am interested in attending training to update my computer skills.
- 18. I consider myself knowledgeable about computers.
- 19. Information security is important within my organization.
- 20. I find my job rewarding.
- 21. My co-workers take information security seriously.

#### Section 5: Perceived Security Awareness Level

- 22. I am committed to the information security mission of my organization.
- 23. I protect my passwords carefully.
- 24. I backup and secure important information.
- 25. I play an important role in the protection of information within my company.

