

2021

An Empirical Examination of the Computer Security Behaviors of Telecommuters Working with Confidential Data through Leveraging the Factors from Fear Appeals Model (FAM)

Titus Dohnfon Fofung

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd



Part of the [Communication Technology and New Media Commons](#), [Computer Sciences Commons](#), and the [Library and Information Science Commons](#)

Share Feedback About This Item

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

An Empirical Examination of the Computer Security Behaviors of Telecommuters Working with
Confidential Data through Leveraging the Factors from Fear Appeals Model (FAM)

by

Titus Dohnfon Fofung

A dissertation submitted in partial fulfillment of the requirements

for the degree of Doctor of Philosophy

in

Information Assurance

College of Computing and Engineering

Nova Southeastern University

2021

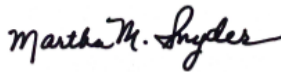
We hereby certify that this dissertation, submitted by Titus D. Fofung conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



Ling Wang, Ph.D
Chairperson of Dissertation Committee

4/14/21

Date



Martha M. Snyder, Ph.D.
Dissertation Committee Member

4/14/21

Date



Junping Sun, Ph.D.
Dissertation Committee Member

4/14/2021

Date

Approved:



Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

4/14/2021

Date

College of Computing and Engineering
Nova Southeastern University

2021

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment
of the Requirements for the Degree of Doctor of Philosophy

An Empirical Examination of the Computer Security Behaviors of Telecommuters Working with
Confidential Data through Leveraging the Factors from Fear Appeals Model (FAM)

by
Titus Dohnfon Fofung
April 2021

Computer users' security compliance behaviors can be better understood by devising an experimental study to examine how fear appeals might impact users' security behavior. Telecommuter security behavior has become very relevant in information systems (IS) research with the growing number of individuals working from home. The increasing dependence on telecommuting to enhance the viability and convenience has created an urgency with the advent of the COVID-19 pandemic to examine the behavior of users working at home across a corporate network. The home networks are usually not as secure as those in corporate settings. There is seldom a firewall setting and lack of an up-to-date antivirus can make home computers more susceptible to attacks – especially when a user clicks on an attachment or malware. The goal of this study was to investigate how the home computer user's behavior can be modified, especially among telecommuters who work with sensitive data.

The data collected using a web-based survey. A Likert scale was used on all survey items with a pre-analysis of the data preceding the data assessment. The Partial Least Square (PLS) was used to report the analysis of the data gathered from a total of 376 response. The study outcomes demonstrated that response efficacy, self-efficacy, and social influence positively influenced protection motivation. The perceived threat severity positively affected both response efficacy and self-efficacy, while the perceived threat susceptibility did not affect both response efficacy and self-efficacy.

The Fear Appeals Model (FAM) extension with computer security usage showed the positive significance of protection motivation on computer security usage. This study adds to the awareness and theoretical suggestions to the current literature. The results disclose the FAM capability to envisage user behavior established on threat and coping appraisals from home computer security usage. Furthermore, the study's FAM extension implies that telecommuters can take recommended responses to protect their computers from security threats. The outcome will help managers communicate effectively with their telecommuting employees to modify their security behavior and safeguard their data.

Acknowledgments

I would like to express gratitude and deep-rooted appreciation to my dissertation chairperson, Dr. Ling Wang, for the support and guidance throughout the process. I could not have achieved the various objectives without her effective supervision. Dr. Ling Wang is a remarkable professor to be admired.

I would not have reached this final point devoid of my dissertation committee members, Dr. Martha Snyder, and Dr. Junping Sun's valuable contributions. Dr. Martha Snyder's immense knowledge and exceptional attention to detail need to be commended. Dr. Sun's awareness of the literature and APA format was very beneficial. I was extremely fortunate to have such great faculty members on the committee to steer my work.

I would like to recognize my late parents, Mr. Fofung Ndahlein and Christina Kahlang Ndahlein, who cannot witness this accomplishment. They ingrained in me the value of education and hard work. I would also like to thank my wife, Relindis, and my children Gurb, Babila, and Nadia, for tolerating the divided attention I sometimes displayed during this academic pursuit.

.

Table of Contents

Abstract iii

List of Tables Error! Bookmark not defined.i

List of Figures Error! Bookmark not defined.ii

Chapters

1. Introduction 1

- Background 1
- Problem Statement 4
- Dissertation Goal 9
- Research questions and Hypothesis 12
 - Research Questions 12
 - Hypotheses 12
- Relevance and Significance 18
- Barriers and Issues 18
- Assumptions 19
- Limitations 19
- Delimitations 20
- Definition of Terms 20
- Summary 22

2. Literature Review 24

- Overview 24
- Theoretical Foundation 24
 - Protection Motivation Theory (PMT) 27
 - Fear Appeals Model (FAM) 28
 - Threat 29
 - Efficacy 30
- Computer Users at Home 31
 - Threats and Vulnerabilities 31
 - Commerce and Finance 33
 - Healthcare Industry 35
 - Past Literature and Gaps 36
- Weakest Target in IS 45
- User Security Noncompliance 46
- The Social Influence in IS 47
- Analysis of the Research Methods 48
- Summary 49

3. Methodology 50

- Overview of Research Methodology/Design 50
- Research Method 51
- Instrument 52
- Ethical Consideration 59
- Population and Sample 60
- Power Analysis 61
- Pre-analysis Data Screening 62

Data Analysis Strategy 63
Presenting the Results 63
Resource Requirements 64
Summary 64

4. Results 66

Pre-Analysis Data Screening 66
 Mahalanobis Distance and Box Plot 68
 Normality and Scatter Plot 68
Data Analysis 69
Instrument Reliability and Validity 71
Findings 76

5. Conclusions 80

Discussion 82
Limitations and Future Studies 90
Summary 90

Appendices 93

A. IRB Approval 93
B. Descriptive variables 95
C. Mahalanobis Distance and Stem & Leaf Plot 146
D. Rerun of Mahalanobis Distance and Stem & Leaf Plot after 8 extreme values deleted 151
E. Normality and Scatter Plot 160
F. PLS Analysis with Factor Loadings 172
G. PLS Analysis after deleting outlier 173
H. Model fit, Reliability, Validity, Coefficient and Outer Loading 174
I. Descriptive variables 183
J. Significance with Bootstrapping 194
K. PLS Analysis with Factor Loadings 197
L. Survey 198

References 216

List of Tables

Tables

1. Constructs Items and Instrument Source 55
2. Instrument Reliability and Validity 72
3. Model Fit and Accepted Values 72
4. Inter-Item Correlations Matrix 73
5. Discriminant Validity 75
6. Summary of Hypotheses Tests 78

List of Figures

Figures

1. Research Model 11
2. PLS Analysis Result for Computer Security Usage 77

Chapter 1

Introduction

Background

With the challenges of the COVID-19 pandemic, there is an increase in individuals working away from their usual protective office setting. The surge in the number of telecommuters has increased the concern about information security of home computers. The weakest links in information security are computers at home that connect to the Internet (White et al., 2017). Home computers are generally not as well protected as those in corporate offices. More corporate work is being carried out in home offices, and these computers require extra computer security precautions; consequently, corporate managers need to be worried about home computer security (Mills & Sahi, 2019). Computer users at home are increasingly using their computers to store and manage sensitive personal and financial data (White et al., 2017). Home computers can be used to stage attacks, such as denial-of-service attacks, against other computers connected to the Internet (Symantec Security Response, 2016).

The new capabilities of home technologies may be exposed to new security threats. There is a need for an approach to secure devices at home and to understand the potential threat to the telecommuter. Studies could commence by recognizing the significance of computer security in the household of telecommuters working with confidential data. In the impending years, it will become more vital to improve computer security for telecommuters and home users in general. Institutional and human factors could be a useful way to relate to protective behavior at home (Mills & Sahi, 2019). The human factors which are relevant to protective behavior can lower security incidents or victimizations.

Computer security breaches and the damages that come with it are moving companies to implement security mechanisms. Though high-tech controls are essential, computer security is also contingent on an individual's security behavior, so it is significant to examine what impacts a user to exercise computer security (Dupuis et al., 2016). The telecommuter will need to abide by organizational security to maintain the integrity of their data. Yazdanmehr and Wang (2016) agree that the main threat to information security is established by careless employees who do not comply with information security guidelines and measures of companies. To address the non-compliance problem by employees, there is a need to promote some approaches that will enhance information security policy acceptance of employees.

Companies require direction in creating an information security awareness or applying an acceptable information security culture for their telecommuting employees (Yazdanmehr & Wang, 2016). The universality and convenience of the Internet have provided enormous social benefits by bridging communities and destroying geographic boundaries. Technological advances have erased the borders between far and wide communities. Communication via the Internet without any boundary has pried open new doors for crime and fraud, thereby exposing millions of home computers to cybercriminals all over the world. To increase this problem further, attackers strategically pick the soft targets like a home computer to improve their chances (White et al., 2017), which implies that the home computer needs to be further protected.

The new capabilities of home technologies are potentially exposed to new security threats (White et al., 2017). A strategy is needed to secure devices in the home and to understand the potential risks involved with the home computer. The approach begins with recognizing the significance of computer security in the household of telecommuters. In the forthcoming years, it

will become increasingly more vital to improve computer security for the telecommuter, and the home user in general.

According to Meroño-Cerdán (2017), the potential of working at home can boost both the quality of life of employees and organizational effectiveness. However, home computers have evolved into a perfect breeding ground for hacking, dispensing, or holding privileged information for ransom (Li & Siponen, 2011). Computer users do not always follow the guidance of experts to take measures to protect their devices, thereby ensuring computer security issues at home (Li & Siponen, 2011). It is vital to examine the home setting and realize how to motivate people to take steps to protect their home computers. Organizations are also challenged with the issues of data security during telecommuting. The security of data has been a big problem for organizations recently. Organizations are very cautious with their data, especially when it is confidential or of a sensitive nature.

Some recent studies employed the Protection Motivation Theory (PMT) to discover these practices (Crossler & Bélanger, 2014). PMT (Rogers, 1975) has its origins in research related to Fear Appeals that are primarily focused on how fear-arousing communication can influence attitudes and subsequent behavior. PMT addresses the issue by breaking down fear appeals into multidimensional components that would allow the researchers to determine standard variables affecting the change of attitude (Milne et al., 2000).

Protection Motivation Theory (PMT) (Rogers, 1975; Rogers, 1983), is a framework, assumes that the inspiration to protect oneself from risk is associated with the subject's cognitive belief on the ensuing features: the severity of the threat, the susceptibility of the threat, the efficacy of coping response in preventing the threat, the cost of response, and the skill to carry out the coping response. The PMT was a suitable behavioral paradigm that might be applied to

assess the handling of computer security technologies. Fear Appeals Modeling (FAM), such as PMT, have been utilized to examine the behavior of individuals. Fear Appeals are used in ads to convince people to buy a product by scaring them about what could occur if they do not.

Considering that the FAM has been applied to the study of an individual's behavior towards policy and instruction compliance, this study attempts to examine how response efficacy, self-efficacy, and social influence (the three main elements of FAM) impact the computer user's behavior. Because threats to computers and computer networks are of concern, the FAM is beneficial to the study of computer user's behavior concerning computer and computer network security.

Problem Statement

Numerous studies have been conducted on user information security behavior. However, most research in computer information security behavior has usually focused on employees in the office setting of an organization (Crossler et al., 2013). Furthermore, few studies have been conducted with home computer users concentrating on information security behavior (Crossler et al., 2013; McGill & Wang, 2017; Menard et al., 2017; White et al., 2017). The home office user or telecommuter working with confidential data certainly presents some security challenges compounded by a lack of up to date antivirus software and no installed firewall. Thus, the current study aimed to bridge this gap by probing the motivation of individuals to protect their home computers from threats when working from home with access to sensitive data.

Some of the challenges are that home computers have become a perfect breeding ground for hacking, dispensing, or holding sensitive information for ransom, and the security cost of mitigating these incidents is astronomical (Johnston et al., 2015; Menard, Gatlin, & Warkentin, 2014; Mills & Sahi, 2019). Therefore, the erratic behavior of home users, such as clicking on an

email link, may lead to security issues like releasing a virus or launching a dangerous website (Öğütçü et al., 2016). The use of firewalls is prevalent in the organizational environment compared to the home setting since the configuration may require some technical expertise, which will introduce an additional financial burden. Most home networks cannot easily fend off or block malware attacks compared to the corporate ones, so the actions of users on a home network are critical to prevent these incidents from occurring.

Information security (IS) awareness programs are intended to increase users' awareness of a threat and motivate them to adopt a recommended response behavior like not clicking on dubious links and install anti-spyware software. Information security researchers have developed several models examining how users respond constructively to IS security threats, for example, installing anti-virus software, firewalls, system updates (Anderson & Agarwal, 2010; Boss et al., 2015; Hanus & Wu, 2016), changing passwords (Workman et al., 2008), and adopting anti-spyware software (Johnston & Warkentin, 2010; Lee & Kozar, 2008). However, it is critical to understand that all these behaviors are instances of adaptive coping known also as danger control, threat avoidance behavior, or problem-focused coping (Hanus & Wu, 2016).

Therefore, we cannot have a comprehensive understanding of workplace anti-spyware software protection without an understanding of behavior concerning spyware on home computers. This is important because employees personally own storage media, such as thumb drives, mobile devices, smartphones, and tablets. There has been limited research focusing on home or personally owned computing security behavior (Anderson et al., 2010; Hanus & Wu, 2016), which implies we know less about user security behavior in the home context than in the business context (Liang & Xue, 2010). While technology answers are accessible to identify and avoid security susceptibilities, software, and hardware solutions alone are not enough since

employee behavior represents the greatest threat to effective information security. Organizations cannot merely advise staff to be aware of security policies and practices. Practical awareness training is a result of engagement through training in which the awareness of computer users is increased, and users across the organization realize that security is the responsibility of everyone (Hanus & Wu, 2016).

Various models examine how individuals respond to threats and take protective steps (Weinstein, 1993), however, in connection with understanding behavior in the cybersecurity and online safety realm, the Protective Motivation Theory (PMT) has been widely used (Boss et al., 2015; Hanus & Wu, 2016). Generally, PMT-based behavior results from a cognitive process (Doane et al., 2016), while habit is an automatic behavioral reaction activated by a situational stimulus devoid of cognition (Chen et al., 2013). Therefore, when sustainable behavior is repeatedly accomplished and turns out to be habitual, the need to engage in the cognitive process will be concealed (Hanus & Wu, 2016). While the rational and cognitive approach to decision making by computer users is the dominant approach, over time, researchers have realized that this is a severely limited approach, in that it does not take into account emotional and affective factors in human behavior (D'Arcy & Lowry, 2017). It has taken some time for the affective aspects, such as fear, alluded by the Fear Appeal articles of Johnston and Warkentin (2010) and Johnston et al. (2015) to appear. They drew attention to the point that most of the choices that people make in their daily working lives, in the context of information system security, are made from habit. Also, increasing anxiety leads to more functional behavior. The previous assertion is in line with results obtained from the Fear Appeal Models (Wall & Warkentin 2019), where threats were found to lead to more compliance.

Straub (1990) argued that stressing the sanctions for information security policy (ISP) non-compliance can help reduce violation of ISP by employees. Numerous studies later proved the effectiveness of sanctions in motivating ISP compliance by employees (Herath & Rao, 2009a; Herath & Rao, 2009b; Hovav & D'Arcy, 2012; Johnston et al., 2015). Studies have also shown that organizations can utilize other measures, such as procedural countermeasures like security policies, technical monitoring, and auditing, to increase the perceptions of sanction severity and certainty of employees, which could further deter security violations (Hovav & D'Arcy, 2012).

McGill and Thompson (2017) observed variations in security perceptions of home computer users and their mobile devices in the United States. The study was focused on mobile device security and articulated the problems of home users not reading security messages or choosing to disregard them. Concerning Fear Appeals, McGill, and Thompson (2017) posit that while social impacts on security behavior are significant in the framework of personal computing, they did not find variations in security behavior levels between mobile devices and home computer users. The users were not obliged to take protective actions on either their computers or mobile devices because of the perspective of others (McGill & Thompson, 2017).

Menard et al. (2017) examined user motivations in protecting their computers by comparing motivational behaviors using Protection Motivation Theory and the Self Determination Theory, which are the basis of motivational factors. The significance of the findings of Menard et al. (2017) is observed through the Fear Appeals message on user security behavior. Although Menard et al. (2017) studied both home and company office users, they did not separate the results according to these two groups. Hence, their study gives impetus to this research because they did not investigate home computer users as a specific population. Also,

Menard et al. (2017) suggested that future research related to one's enthusiasm to carry out protective behaviors on one's data should involve a distinct measure of motivation. This conclusion corroborates the need for a study like this research since it included telecommuters working with confidential data. The motivational features of Fear Appeals communication would be considered when the telecommuter was confronted with the implementation, or lack of enforcement, of computer security safeguard mechanisms on their computers.

Another study on home security was done by Mills and Sahi (2019) based on the implementation of extra security measures on home computers and laptops without testing a comprehensive model of PMT. The study called for an extension of the current model by involving other factors such as fear, attitude, and descriptive norms that might likewise influence behavior. These research findings also gave credence to the need for the study using Fear Appeals with telecommuters working with sensitive data. Since the study was done in New Zealand, the results may not extend to other countries, and the general public sees the overall Internet or network security as an essential issue (Mills & Sahi, 2019).

The method of persuasive communication has been established as an effective way of communicating with staff in the office setting to convince them to follow the correct security protocol (Johnston, Warkentin & Siponen, 2015). The use of Fear Appeals has not been widely studied with users in the home computer security environment (Crossler et al., 2013). This research intended to study the habits of telecommuters to determine if the use of Fear Appeals would modify their behavior about computer security actions while working with confidential data.

Dissertation Goal

This research intended to bridge the literature gap between the home office and organizational setting users by examining people's motivations to protect their computers from threats, especially when working with confidential data from home. The study explored how the Fear Appeals elements of response efficacy, self-efficacy, perceived threat severity, perceived threat susceptibility, and social influence are associated with security behavior of telecommuters as they work with sensitive data. Fear Appeals are a vital concept because it is how computer security providers predominantly choose to communicate with users (Boss et al., 2015). An example of a Fear Appeal communication is people at work being notified of severe consequences if they choose to disregard a company policy (Puhakainen & Siponen, 2010).

The telecommuters are neither necessarily bound by corporate policies nor the related fear of the consequences of breaching corporate policies while working from home. It does not follow that the home computer user does not fear the consequences of unacceptable computer security behavior (White et al., 2017). Nevertheless, their consequences are personal and not due to corporate policies or fear of workplace ramifications (White et al., 2017). However, computer security providers, who principally use Fear Appeals to impart sound computer security habits, do not distinguish between home and office computer users when communicating with users (Willison et al., 2016). Hence, what was not known was whether Fear Appeals impacted home computer security. The current study investigated the effect of Fear Appeals communication (as determined by response efficacy, self-efficacy, perceived threat severity, perceived threat susceptibility, and social influence) on the security behavior of a telecommuter working with confidential data.

There is a mounting indication that hackers exploited the current fears about the COVID-19 virus to target people who are increasingly working beyond the protected confines of their office settings to exploit their cyber susceptibilities. The COVID-19 pandemic fears have fueled a rush to work from home, and thereby escalating the number of telecommuters accessing sensitive information over their company's network. The surge in information breaches affecting computer users had increased the need to examine this dilemma, especially when accessing sensitive information while working from home.

The current study proved, along with preliminary information, the rationales that added to the information security practices of telecommuters from the perspective of security behavior. In particular, the objective of the investigation was to ascertain the impact of the independent variables (i.e., perceived threat severity, perceived threat susceptibility, social influence, response efficacy, self-efficacy, and protection motivation) on the dependent variables (i.e., telecommuter security behavior as it relates to the protection of confidential data). To achieve the current study objective, a research model, and the subsequent hypotheses was initiated on the links between the constructs. The research model was centered on concepts from PMT and FAM (Figure 1). As shown in Figure 1, the model is an expansion of the risk control process as defined by PMT and FAM (Johnston & Warkentin, 2010). The justification for leveraging the FAM and PMT is their capacity to predict user security actions using cognition to realize the activities that facilitate transformation in them (Herath & Rao, 2009). The security behavior and judgments of telecommuters are centered on rationale and judgment as a rule of thumb, and the cognitive issues affect information security behavior of users and their conformity or non-conformity in their judgments.

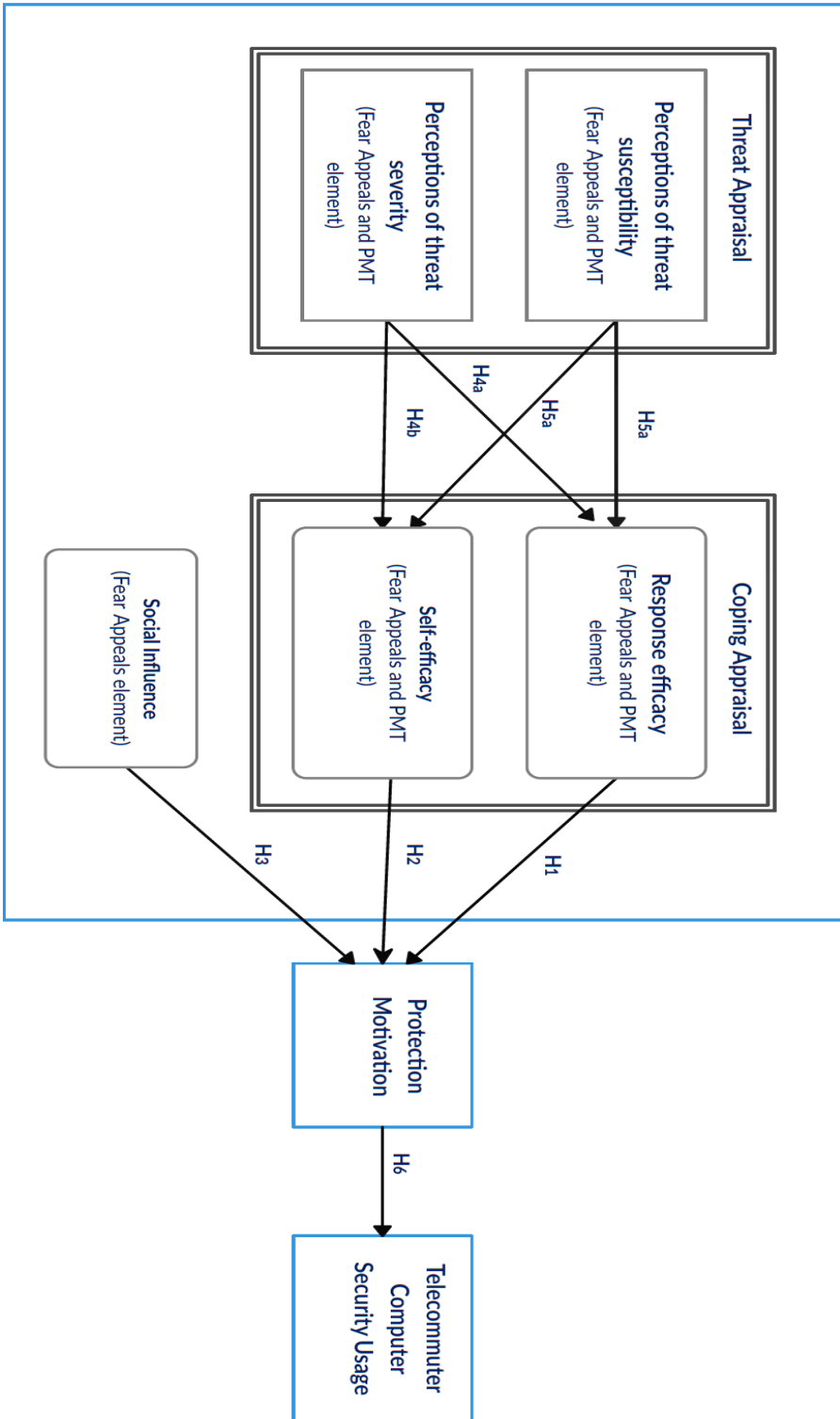


Figure 1. Research Model

In situations where the Fear Appeals is effective in provoking a considerable awareness of the threat, an assessment of the response efficacy and individual's capacity to perform the response (self-efficacy) instantly ensues. While in circumstances where a threat is perceived and supplemented by a modest-to- elevated degree of perceived efficacy, people will act to mitigate the threat (Johnston & Warkentin, 2010). Though the FAM and PMT have been employed in a variety of information security situations, no study has been carried out using the paradigms and approaches on telecommuters working with confidential data. As such, the current study seeks to be a practical replication, in which these theories, techniques, and suppositions are embraced from the initial study.

Research questions and Hypothesis

Research Questions

RQ: To what degree do self-efficacy, response efficacy, threat severity, perceived threat severity, perceived threat susceptibility, social influence, and computer security protection motivation impact the security behavior of a telecommuter working with confidential data?

Hypotheses

The study's intended model conveys the two aspects of perceived efficacy, response efficacy, and self-efficacy as direct intent elements. Response efficacy indicates the extent to which a person believes a suggested response will successfully avert a threat (Rogers, 1975; Witte, 1992). Assessments of response efficacy are a cognitive process in which people form opinions about the usefulness of a recommended response-ability to avoid a threat (Witte, 1992). Eventually, their perceptions of response efficacy will ascertain how they decide to handle the threat (Rogers, 1983). Corresponding to PMT, modest to elevated levels of response efficacy is

related to positive tendencies of threat mitigation while a recommended response is endorsed. A telecommuter considering whether he or she will embrace a suggestion to protect against spyware will install and use anti-spyware software. The telecommuter will consider the capabilities of the anti-spyware resolution and form an outlook toward the advice based on this appraisal. It was due to this backdrop that the following hypothesis was developed:

H₁: Response efficacy will have a positive effect on a telecommuter's computer security protection motivation.

Excessive levels of emotional awareness are believed to have a negative effect on self-efficacy (Lazarus & Folkman, 1984; Marakas et al., 1998). High levels of emotional stimulation, such as that presented by a perceived threat to the security of their digital assets, resulting in reduced levels of perceived ability to use a computer, as stated by Marakas et al. (1998).

Menacing events, such as viral attacks, Trojan activities, and spyware infestations, are perceived as more severe or probable, a telecommuter may begin to doubt their capability to function sufficiently within the delicate threat conditions without causing harm to data or their computing environment. More, Gutek and Winter (1990) contend that high levels of emotional stimulation are linked to reduced computer user's performance.

Like the way an individual cognitively evaluates the efficacy of a response, a person also appraises the capability to execute the recommendation (Maddux & Rogers, 1983; Witte 1992). Initially established by Maddux and Rogers (1983) and Rogers (1983) as an expansion of PMT, self-efficacy was seen as the contributing factor of intent concerning a recommendation to handle a threat. When considering a telecommuter's decision whether to endorse a recommendation to avoid spyware invasions, though he or she thinks the supported response is

effective, the telecommuter will have to contemplate his or her ability to install and run the anti-spyware solution effectively. Based on this argument, the following hypothesis was developed:

H₂: Self-efficacy will have a positive effect on a telecommuter's computer security protection motivation.

A person's eagerness to use new technology is the extent to which the person perceives his or her coworkers and others whose views matter backing its acceptance and use is a major factor (Sharma et al., 2014). This factor is referred to as social influence, which has a prolonged record and has lately been put in a broader perspective as part of technology acceptance literature. Social influence is strongly associated with social norms, which were established to be a considerable factor of behavioral intent in the concept of reasoned action (Fishbein & Ajzen, 1975) and the idea of planned behavior (Ajzen, 1991; Venkatesh & Davis, 2000). In those concepts, it was determined that an individual's behavior is inspired by the extent to which prominent people support or reproach the outcome of behavior (Venkatesh et al. 2003). Likewise, social influence links to Thompson et al. (1991) concept of social factors. They discussed an individual's opinion of the reference group's subjective culture and precise social agreements that the person has made with other social situations (Venkatesh et al. 2003). Ultimately, social influence is intimately linked to Moore and Benbasat (1991) construct image, which refers to the extent to which the use of an innovation is perceived to strengthen one's social position within his or her peer group.

The study contented that telecommuters would engage in specific discussions as well as indirect activities concerning the proper actions to take on the security of their communications. Venkatesh and Davis (2000) suggested that the justification for the direct result of social influence on behavioral intent was that people elected to behave, though they were not

themselves in favor of the behavior or its consequences. If people think one or more significant contact persons believe they should act in a certain way, they are motivated to comply with the contact persons.

The contact persons of interest may be a peer, at the very minimum. Likely, those accountable for security inside an organization will often give guidance and alerts to the users inside the organization on how to operate their computers securely. While this support is provided inside a company setting, it usually comes from employees in positions of authority and accentuates compliance with perceived standards within the firm. More, Lewis, Agarwal & Sambamurthy (2003) stated that if a peer, supervisor, or some other actor in a significant social network thinks that technology is helpful, through a process of shared understanding, so will the target individual. It was with this understanding that the following hypothesis was developed:

H₃: Social influence will have a positive effect on telecommuter's computer security protection motivation.

Perceived threat severity was initially pinpointed by Rogers (1975) as the main element of a Fear Appeal that contributes to a person's reaction. Perceived threat severity is the belief that a person involved with Fear Appeals will harbor the significance of the threat (Rogers 1975; Witte 1992). PMT defines assessments of threat severity to be the ability to control the intensity of response. The assessment is done by clearly controlling perceptions of both response efficacy and self-efficacy. For instance, as a computer user's understanding of the severity of a spyware threat rises, ideas about the capabilities of anti-spyware software to effectively address the threat decline (Witte 1992).

Furthermore, discrepancies in the perceived severity of the spyware threat cause computer users to reevaluate their Perceived threat severity was first recognized by Rogers

(1975) as a primary element of a Fear Appeal that influences an audience's reaction. Perceived threat severity is the notion that the Fear Appeals audience holds about the significance of the threat (Rogers 1975; Witte 1992). PMT describes perceptions of threat severity as the ability to control the intensity of response. It does so by manipulating perceptions of both response efficacy and self-efficacy, for instance, as a computer user's assessment of the severity of a spyware threat increases, the opinions concerning the potentials of anti-spyware software to handle the threat decline (Witte 1992) effectively. Also, differences in the perceived severity of the spyware threat trigger the telecommuter to reevaluate their ability to use anti-spyware protection effectively. As the threat is perceived to be extra severe, the telecommuter will feel less able to address the threat effectively. These resulted in the following hypotheses being developed:

H_{4a}: Perceptions of threat severity will negatively influence perceptions of response efficacy.

H_{4b}: Perceptions of threat severity will negatively influence perceptions of self-efficacy.

Perceived threat susceptibility was also adopted by Rogers (1975) in his breakdown of the components of a Fear Appeal as an essential element that impacts a person's reaction to Fear Appeals. According to the logic which prescribes that the perceived severity of a threat influences the ensuing relationships between a user's intent and his or her opinions of response efficacy and self-efficacy, a user's perceptions of the likelihood of encountering the threat also offer such influence (Rogers 1975; Witte 1992). In a study of Fear Appeals in the aspect of AIDS prevention, Witte (1994) found that as persons were given literature stressing the prevalence of the AIDS epidemic, the participants' assessments of their ability to protect themselves from the risk and of the effectiveness of condom use declined. A related study regarding the threat of

contracting a sexually communicated disease yielded the same results; as assessments of threat susceptibility increased, perceptions of efficacy reduced (Witte et al. 1996). In the context of the telecommuter defense, it is expected that opinions regarding an anti-spyware solution to provide safeguards efficiently will decrease in strength as the threat of such an attack becomes more likely. The following hypotheses are developed:

H_{5a}: Perceptions of threat susceptibility will negatively influence perceptions of response efficacy.

H_{5b}: Perceptions of threat susceptibility will negatively influence perceptions of self-efficacy.

In the PMT study, the leading notional emphasis has been forecasting behavior regarding protection motivation (Floyd et al. 2000; Rogers 1983; Rogers & Prentice-Dunn, 1997). Though, beyond information security research, PMT has been effectively broadened to forecast behaviors (Floyd et al., 2000). Therefore, a prominent PMT-based health study assesses real behavioral transformation, not simply intentions (Fry & Prentice-Dunn, 2006; Milne et al., 2000). The current study claims that real behaviors are beneficial for information security study since the objective was to alter security behaviors, not only to improve protection motivation (Crossler et al., 2013). This study, therefore, claims that to enhance conduct of users, an effective assessment of the complete classification of PMT ought to likewise consist of a review of actual behaviors. Consequently, PMT meta-evaluation reveals that protection motivation would be the most significant predictor of behavioral modifications (Milne et al., 2000). Hence:

H₆: An increase in computer security protection motivation improves the computer security behaviors of telecommuters working with sensitive data.

Relevance and Significance

The current study was vital in numerous ways in the field of technology and business. This research plans to study the cyber alertness characteristics of telecommuters. Studies show that these attitudes toward security behavior establish a distinct lack of consideration regarding caution associated with computer security (Shropshire, Warkentin & Sharma, 2015; Wang, Myers & Sundaram, 2013; Willison et al., 2013). This research intended to help organization managers by establishing how the security behavior of telecommuters are influenced when they work from home with sensitive data.

A home computer can be used for personal matters, which include social networking, gaming, as well as logging into work or financial institution websites (White et al., 2017). Therefore, home computer users are concerned with protecting information privacy and security (Geil, Sagers, Spaulding, & Wolf, 2018). In the area of cybersecurity, the Fear Appeals Model (FAM), within the confines of the broader PMT has been used successfully in many settings, including but not limited to health care (Kim & Shin, 2018; Rogers, 1985), academia (Lee, 2011) and marketing (Fox & Royne, 2018). The use of the Fear Appeals elements of self-efficacy, response efficacy, threat severity, perceived threat severity, perceived threat susceptibility, and social influence regarding home computer security behavior, can be applied to the society at large using the PMT to engage their corresponding audiences.

Barriers and Issues

A web-based survey method was used to gather quantitative data from the participants. The participants were adult telecommuters working with confidential data. Crucial obstacles in this method included attaining a reasonable sample size, the eagerness of the participants to contribute to the study, and how the study could be extended to others. Obtaining the right

sample for research was challenging. Consequently, the participants were recruited via professional associations and professional groups. The respondents were chosen randomly from the population of telecommuters working with sensitive or confidential data. Furthermore, assessing security behavior in a group could be demanding, since security concerns might differ from person or group. Also, the focus was on users working from home and accessing sensitive information.

Assumptions

It was presumed that the telecommuters are responsible for the security of the computers they use, and hence this study accepted that irrespective of the computer security devices, they were exposed to human mistake and negligence. Since data collection was carried out utilizing an online survey, a cloud-based software service company, SurveyMonkey™, was used. It was assumed that the data gathered were demonstrative of the population stated and that the survey respondents could take the provided surveys. Also, the study relied on the participants giving accurate self-reported data.

Limitations

Anytime there is a survey that requests information to be self-reported, there is a chance for the participant to avoid embarrassment, give socially acceptable answers, and perhaps slightly alter their responses to what they believe they should be, rather than what they are. The possibility of the respondent's answers may stray from the norm because of how the respondent interprets the question, or how suitable the response is measured due to their level of experience (Page & Uncles, 2014).

Delimitations

Some studies show that it may not be a case of a social appeal, but perceived levels of confidentiality and privacy that could lead to false answers of behavior on a survey (Laajasalo et al., 2016). People may lie to get a sense of elation or thrill, known as conning delight (Clements et al., 2016). These are examples of established concerns when data was collected via a survey, and it was presumed such an issue did not skew the collected data. The survey instrument used presents several minor imperfections. First, the population was telecommuters working with sensitive data, and how long the recipient has been using a home computer. Though, the period of a home computer did not necessarily correlate with the expertise in using a home computer; it was reasonable that some telecommuters who have been using a computer for a long time were not skilled with computers.

Definition of Terms

The terms utilized in this research and their descriptions are provided below:

Construct - Trait or attribute that can be quantified or monitored, and that fluctuates between persons or groups being examined (Creswell, 2008).

Construct Items - research questions given to survey respondents to assess or research a construct (Monroe, 2000).

Denial of Service Attack - An attack where unwarranted system calls are utilized to devastate the processing capability of a target site or its routers (Chowriwaret al., 2014).

Fear Appeals Model - A type of persuasive communication that utilizes fear as a way of altering the recipient's behavior (Witte as cited in Njoroge & Mberia, 2014).

Malware - Malicious software that was designed to cause damage or devastation (Goldsborough, 2014).

Information Security - Process to guarantee the privacy, reliability, and ease of use of information (Bishop, 2003).

Information Systems (IS) - A combined cluster of processes in a user-computer setting that runs on structured data and is intended to simplify the informational desires for the executive and operation of the company (Torres-Perez & March-Chorda, 2002).

Persuasive Communication - This is a type of communication used to encourage people in the academic and psychological study (Taniguchi et al., 2014).

Protection Motivation Theory - A type of persuasive communication that utilizes enticement to people's intrinsic inspiration as a way of altering the recipient's behavior (Njoroge & Mberia, 2014).

Response Efficacy - The idea that a type of response is the appropriate one to avoid an unfavorable outcome (Rogers, 1975).

Self-Efficacy - The idea that a response from a person will help in averting an undesirable result from a particular threat (Sommestad et al., 2015).

Security Behavioral Intentions - The intentions of a person to respond to a presented situation with a particular response (Lee & Larsen, 2009).

Social Influence - The responsibility or belief from social groups that can change an individual's response to a given situation to execute measures that are anticipated of people/groups that favor a specific result (Lee & Larsen, 2009).

Spyware - Software that is developed to gather user's information about a user without their knowledge (Lavesson, Boldt, Davidsson, & Jacobsson, 2011).

RESP - response efficacy acronym in the survey construct.

SEFF - self-efficacy acronym in the survey construct.

TSEV - threat severity acronym in the survey construct.

SINF - social influence acronym in the survey construct.

TSUS - threat susceptibility acronym in the survey construct.

ATT – attitude acronym in the survey construct.

PM – Protection motivation acronym in the survey construct.

CSU - Computer security usage acronym in the survey constructs.

PERP - Performance expectancy acronym in the survey construct.

Summary

The background of the study focused on a research-worthy problem in the context of user security behavior. It was precisely based on the information security behavior of computer users from the perspective of data breach and malware. The problem statement recognized and expounded on the problem to be examined, why it is a problem, and the way this problem has become relevant. The recognition of the goals proceeded with the problem statement. The research question was presented to denote the areas in the literature that were considered. The research model was established on the research question and the ensuing hypotheses. The research model was based on the FAM and the PMT constructs of self-efficacy, response efficacy, threat severity, perceived threat severity, perceived threat susceptibility, and social influence impact as determinants of security behavior of a telecommuter working with confidential data.

The relevance and significance were provided to further expand on why it was essential to explore the problem, earlier efforts made at assessing the problem, and the significant distinction in the impact of the study to realize the solution to the problem. Similarly, barriers

and issues encountered in an endeavor to recommend some answers to the problem detected was demonstrated. Last, assumptions, limitations, and delimitations of the research were presented.

Chapter 2

Literature Review

Overview

Many research attempts have been dedicated to improving technologies that may possibly safeguard information security. Technical answers could be beneficial, but the fundamental principle of these answers is based on the perception of users averting risky behaviors (Du et al., 2013). Increasingly, various researchers devote significant attempts to the advancement of security consciousness and risk communication plans to improve the awareness of users regarding safe computing habits and security risks. User behavior in information security, however, is a complex area of research because it is not easy to adopt one standard characterization of what represents intended computer user behavior. The planned user behavior cannot be readily projected and is complicated to control (Alhogail et al., 2015).

The literature review was centered on integrating literature from previous research and sources that have strived to assess the user behavior concept in information security. The literature review assessed prior studies for their concepts, theories, contributions, limitations, and gaps, also evaluated the methods used in the study. The chapter sought to comprehend malware and data breach and the circumstances involved in the information security behavior of users at home.

Theoretical Foundation

The theoretical foundation was based on Johnston and Warkentin's (2010) FAM, which stemmed from Rogers' PMT (Rogers, 1975; Rogers, 1985). The concept of Fear Appeals has been used for a while to persuade individuals to carry out the anticipated action, mainly when employed in IT information security (Jenkins et al., 2014). Hence, FAM is entrenched in the

concept that cognitive processes and fear impact persuasion, in which individuals can be manipulated to protect themselves from an array of physical, psychological, and social perils (Williams, 2012). In FAM, people focus on two unique activities, called threat appraisal and coping appraisal. Throughout the threat appraisal stage, people examine the severity of the threat and its susceptibility, while in the coping appraisal stage, people investigate the response and self-efficacy to counteract the threat (Johnston & Warkentin, 2010).

Founded on underlying and resulting variables embraced in the Fear Appeals Model (FAM) and enhanced with backgrounds of technology-reliant behavior, the use of the FAM was proposed. The FAM has been successfully replicated and extended both in IS research (Johnston et al. 2015; Johnston et al. 2019) and in marketing (Orazi & Pizzetti, 2015), using different contexts, populations, and estimation methods. The FAM describes a user's participation in individual computer security activities suggested in fear-inducing persuasive communications. The study incorporated social influence as a construct with PMT since it has been shown to improve behavioral security studies (Orazi et al., 2019). Social influence is involved in the model as an explicit determinant of behavior and helps in predicting the use of specific security technology. Perceptions of threat severity and susceptibility are placed as direct antecedents of response efficacy and self-efficacy and implicitly impact behavior. Behavior is directly affected by perceptions of response efficacy, self-efficacy, and social influence (Johnston & Warkentin, 2010).

The threat alternative requires one in which independent telecommuters accessing sensitive data would be able to take actions to mitigate. Some significant attention has been given to the risks and approaches for the mitigation of spyware. Spyware is a particularly complicated form of malicious code that can infect a computer and compromise not only the

functionality of the resource but likewise the privacy of the user and the data they access (Johnston & Warkentin, 2010). Furthermore, these infections can happen without the approval or the consent of the user; in this situation, the software can carry out unnoticeable surveillance and reporting of the computer user's computing activities.

There are new and more menacing threats to computer user information resources each year. These are the threats that sanction persuasive communications (Fear Appeals) to computer users because companies have yet to institute practices for adequate defense, or because users are not meticulous in their approach to protect themselves. Spyware and data breaches provide suitable substitutes for those sorts of threats. The objective of Fear Appeals is to improve perceptions of threat and efficacy irrespective of any presumptions the Fear Appeals audience may have held regarding the threat before experiencing the Fear Appeals message. If the Fear Appeal is efficient, perceptions of threat and efficacy was improved enough that the computer users bound to follow the recommended response (Johnston et al., 2015).

Johnston and Warkentin (2010), analyzed the effect that the Fear Appeals concept has on computer users in terms of information security and computer security. The effect of fear appeals on computer users to assess their reactions against different types of security threats was explored. The investigators particularly examined how computer users handle the malware risk. The research was carried out using experimental methodology centered on the protection motivation theory. A sample of 311 staff members, faculty, and students was chosen for study in a university setting, and 275 useful surveys were conducted and examined. The participants included 61% males, of which 73% were age 18-29 years. The increased number of network attacks like viruses, insider abuse, breaching networks, and unauthorized access were discussed in Johnston and Warkentin's (2010) study. The data revealed that not only the attacks continue to

increase but also their degree of complexity and effect (Johnston & Warkentin, 2010). The study analyzed computer users in a decentralized and non-corporate setting. Such users, individually or jointly, were held to maintain their systems and were expected to benefit from the processes, which correspond to their company's objectives. This form of sampling was suitable to assess the level of persuasive communication within the business environment.

Protection Motivation Theory (PMT)

Earlier research had used many theories to assess protective behaviors. These involve the Theory of Planned Behavior, the Theory of Reasoned Action, and the PMT (Lebek et al., 2013). Using these theories, PMT is exceptionally pertinent since it explicitly considers a threat and an individual's ability to handle it. With its roots in the field of healthcare, PMT was established to detect the cognitive processes that a person encounters when subjected to a threat (Rogers, 1975). In the concept of PMT, protection motivation occurs from the contemplation of a possible threat and individual's wish to elude the consequences of the threat. This includes two main reasoning processes: a threat appraisal and a coping appraisal. The threat appraisal finds and assesses the threat in terms of the perceived severity of and susceptibility to the threat, combined with an individual's evaluation of the rewards that may occur from not taking protective actions. It follows that even if a threat is recognized as probable and its effect is severe if the incentives for not acting are extreme enough, this will counteract the protective action (Mills & Sahi, 2019).

When a person evaluates the threat, the coping appraisal ensues. This comprises an assessment of response efficacy, self-efficacy, and response costs. Response efficacy is the perceived effectiveness of diminishing the threat, whereas self-efficacy is a person's confidence in carrying out the countering protective action as opposed to the threat (Rogers, 1975). The response costs are the costs sustained when executing the protective behavior, such as money,

time, and operating cost (Jansen & van Schaik, 2017; Rogers, 1975). In summary, the response efficacy, the coping appraisal, and self-efficacy should be higher than the response costs for a protective action to be undertaken (Rogers, 1983).

Fear Appeals Model (FAM)

Johnston and Warkentin came up with the FAM in 2010. The FAM offers a streamlined layout of the various features of the standard PMT constructs with the addition of the social influence variables in theory. The FAM likewise takes a different approach to tackle the relations amongst threat and efficacy via factors such as severity and susceptibility as the direct predictors. The FAM was framed to form a cohesive model that combined parts of the PMT with other theories. The FAM is comparatively recent and, in numerous situations, is misconstrued for the PMT (Boss et al., 2015).

The FAM is often seen as a form of persuasive communication that concentrates on the negative consequences or probable punishment that can be the outcome of a course of action. When Fear Appeals are used as a threat or an effort to scare people, it can lead to adverse outcomes. When Fear Appeals are employed as a challenge, the consequences can be very positive, as indicated by a study conducted by Putwain et al. (2015).

Fear Appeals can be most productive by stressing the adverse outcomes of individual action to convince the person to avoid that outcome. It illustrates how self-efficacy, response efficacy, and social influence are used in combination with threats and susceptibility to form a theory like the PMT. The PMT has been mostly used in healthcare studies and has been fine-tuned for users to modify their behavior. PMT is one of many frameworks employed in the business environment. This concept was established by Rogers to explain the use of Fear

Appeals (Rogers, 1975). The outcome became an approach that was revised to work directly, countered to being revised to work with Fear Appeals.

The PMT uses two exclusive processes to evaluate Fear Appeals: threat appraisal and coping appraisal (Ruiter et al., 2014). Threat appraisal discusses issues associated with the severity of a threat and how vulnerable a person is to that threat. The coping appraisal is about determining the usefulness of the response, dubbed response efficacy, and how effectively an individual can implement the response (Njoroge & Mberia, 2014; Ruiter et al., 2014). Coping appraisal signifies both response and self-efficacy as vital and mentioned in a great deal in works associated with the PMT, while severity and susceptibility are threat appraisals (Njoroge & Mberia, 2014).

Threat

The threat is a risk, regardless of its acknowledgment by people (Witte, 1992). When an individual could perceive a threat, the person may be identified as having some perception of the threat (Johnston & Warkentin, 2010). The level of risk increases anxiety and fear among individuals, but the degree of anxiety can differ from one situation to another. The Fear Appeals should not only demonstrate that fear exists but should also warn the user about the risk and seriousness associated with the identified threat. This viewpoint is widely recognized as a level of risk/threat severity. Another question is whether the individuals think they are the target of the perceived risk/threat (Plotnikoff et al., 2014) or that this threat may not extend to them. Hence, the seriousness of the risk and the susceptibility to the risk are the two elements of Rogers' four mediation processes. The additional two elements are self-efficacy and response-efficacy (Rogers, 1975).

Efficacy

The concept of efficacy is divided into two spin-off groups in the broader context of PMT, which include self-efficacy and response efficacy (Menard et al., 2017). The notion of self-efficacy is that an individual has the potential to adopt the proposed measures against the threats, whereas response-efficacy refers to the belief that the proposed action would reduce the severity of the threat. The principles apply to the current study as computer users make judgments about the protection of their computers founded on the perceived security threats. Computer safety providers rely on self-efficacy as well as on the confidence that the individuals they deal with would take suggested actions to mitigate the associated threats/risks.

In both the fear appeals concept and PMT, efficacy is a repeated phenomenon. Besides, PMT identifies two out of the four elements used for understanding the concept of Fear Appeals. The inclusion of self-efficacy is an essential aspect regarding the amendments that were brought to the motivation theory in 1983. In terms of Fear Appeals, this model is comprised of three concepts: threat, fear, and perceived efficacy (Williams, 2012). Threat and coping evaluations are the foundation of PMT.

Self-efficacy is the presumption that an individual could acquiesce to a proposed deed, whereas response-efficacy assumes that the individual eliminates or removes the threat by implementing the advice and recommendations given to them by the security professionals (Yoon et al., 2012). Self-efficacy also refers to one's willingness to take specific actions to address the potential threat, while response-efficacy is a trust in the process and the principle that the threat can be abated if recommended actions are taken. In the case of spyware, self-efficacy refers to the confidence of a person to take some suggested actions if they discover spyware in the computer system.

Computer Users at Home

Threats and Vulnerabilities

Personal computing was first associated with a home-based desktop and then with a laptop. Today, however, the use of smartphones, tablets, and Bluetooth devices is as typical in homes as personal computers. The current study, as mentioned before, was concerned with the security behaviors of home computer users. From this aspect, the security of a home computer cannot be separated from other devices that we use in a house employing Bluetooth and related technologies. The use of these technologies tends to pose security risks for its users (Ahn & Jung, 2016; Geil et al., 2018).

The weak security of home devices is directly related to the nominal awareness of the users of those devices. Often it is needed to know whether an individual is aware of safety and whether there is a risk associated with their way of using the home devices. It is also essential to know whether the consumer has adequate knowledge of the issues related to cybersecurity (Han et al., 2014). According to Han et al. (2014), security awareness of the home computer user is directly connected to the adoption of security measures. They also found that the threat awareness of users does not have a role to play in the selection of the third-party security application.

Moreover, the authors found that the installation of security apps is directly related to the security awareness and concerns of home users. Such studies prove that the adoption of security measures is based on the increasing level of awareness of computer users. They validate the point that adequate home computer security is directly linked with the level of awareness that home computer users have regarding the need to secure the computer system.

From a software and hardware security viewpoint, technologies like Bluetooth-based systems can pose security risks to the users. The concern is that many people are not willing to take action to reduce the vulnerabilities associated with the use of these devices (Tan & Aguilar, 2012). The threats associated with the use of such devices include penetration risks, location tracking, and identity detection risks. Bluetooth provides as much as three general security services, which include data encryption, authentication and authorization, and data confidentiality. It does this using the passkey that enables the receiver of the message to receive and open the message. Such services can make Bluetooth a robust device, but if security controls are not applied to the services, it can also turn into a severe risk (Tan & Aguilar, 2012).

Instances of the home computer use include sensitive security practices such as email scanning, social media activity, Internet browsing, watching video-sharing as well as unsafe security practices like mortgage/brokerage and online banking. It is logical to envisage a usual home computer user to include parents, children, families, and even friends and visitors who may wish to use the home computers of the people whom they visit (Arachchilage & Love, 2014; Geil et al., 2018).

Moreover, it is reasonable to assume that the average home user of a computer is not an IT expert, although it is not easy to define the kind of standard home computer user. Some might argue that individual family members in a traditional home are much more educated and vigilant about their computers while others are not so educated or are not worried about the safety of the machine. For instance, adolescents are not as cautious as their parents. In a situation where someone utilizes a computer in the home of another individual, it was unlikely that the person would practice safe computer habits. Individual users play a crucial role in safeguarding computer security (Dang-Pham et al., 2016; Gerhart & Windsor, 2017; Zhang et al., 2017). Virus

attacks, ransomware, spearfishing, a phishing email, and all other kinds of incidents on computers are agnostic to the users and owners (Shillair et al., 2015).

It is also essential to keep in mind the indistinct difference in both homes and work computer users when discussing users of home computers. Increasingly, virtualization in organizations is playing a viable role in telecommuting jobs. The spread of Internet technologies allows staff to work from home (Arachchilagea & Love, 2014; Chithambo, 2015). It is irrational to require a person to spend resources for a separate home computer to do business at home unless the employer's requirement is enforced. Understandably, it is rational to assume that working remotely could threaten a computer network in the office, such as accidentally sending an infected file to a person or a work colleague from a home computer (Arachchilagea & Love, 2014; Chithambo, 2015; Geil, 2018). Many reports suggest that people are the weakest component of a computer security network, and this is also a vital argument of the current study (White et al., 2017).

Studies have shown that technology adoption does not imply lower occurrences of computer security issues (White, 2015). In the protection of the computer or computer network, security processes may be adopted, but it is eventually the obligation of the user to abide by the guidelines. Consequently, the problem of security should be considered more as a behavioral rather than a technological issue (White, 2015). In this regard, it is realistic to say that a home computer's safety should also be considered a human factor rather than a technological problem.

Commerce and Finance

The Internet is an outstanding source of information and has several advantages. The most frequent use of the Internet is that it empowers users to purchase merchandise and services online. E-commerce plays a crucial role in enabling users to shop easily using their mobile

devices or the home computer. Many trade dealings are carried out regularly over the Internet. Hartono et al. (2014) indicated that in e-commerce, confidentiality, accessibility, and non-repudiation present the most significant problems. E-commerce is very broad and distributed throughout the world and applies to the possible problems of payments on the Internet. The social, functional, and financial risks are the anxieties for most home computers (Al-Rawad et al., 2015).

About maintaining a corporate website to process business activities online, the diverse experience of fear from the service providers reveals that there are many facets to maintain a website and to make the user at home feel safe. There is a possibility for a security risk or hacking of the home computer machines that online retailers and corporations need to consider. If a person is the focus of a security offensive, a weakness could be their lack of awareness about what is secure and not secure (Geil et al., 2018).

The financial sector specifically refers to banks or financial corporations. To serve their computer users, these businesses cannot only access consumer accounts through the Internet but also promote their use. As a result of these services, they become the typical user (McGill & Thompson, 2017). There are many ways of breaching the network from a provider's point of view that include spyware, spam, viruses, malware, software engineering, web hacking, distributed denial of service, as well as phishing. According to Wang et al. (2013), since financial firms are very dependent on the use of information technology, the data stored is highly susceptible to the network-based attacks. The incidents against these financial institutions may result in wide-ranging social or financial benefits. When stated in an alternative way, once infected, the attacker could unintentionally affect the business by spamming the known email addresses in the organization's database and the organization's client base (Arachchilage & Love,

2014). Therefore, the computer protection of the telecommuter who wants to access a financial website and the protection of the financial company supplying the portal are interdependent.

Healthcare Industry

Patients provide their confidential information to health professionals to seek treatment. Many patients log in through their home computers for this purpose. One of the health sector's problems is the disparity between consumers of health data and suppliers of the data (Manogaran et al., 2017). In research-based on digital access, patient factors, and online behavior, Woods et al. (2017) asserted that both patients and healthcare systems regard digital health care as a significant way to improve patient access and self-treatment. The increasing usage of the patient portals to safely contact healthcare providers, to renew medications, and to get test results and clinical notes are becoming a trend that is not free of the threat of privacy leaks (Woods et al., 2017).

When patients are computer users or clients, their electronic access records are similar to home users who have Internet access to financial data or insurance service. However, in the type of details it holds, the healthcare sector is unique. An individual's medical history is highly relevant and useful. The healthcare sector is governed to the degree that the Health Information Technology for Economic and Clinical Health (HITECH) and the Health Insurance Portability and Accountability Act (HIPAA) are considered separate forms of legislation (Al Ameen et al., 2012). The necessity to safeguard medical information of patients has contributed to the partnership of the cybersecurity and the health security industry. Domestic privacy concerns of users need to be tackled via efficient protection practices (Arora et al., 2014).

Past Literature and Gaps

Previous behavioral information security research mostly requires an explicit presence of actual security use as the dependent construct in their models. Its marginal use in previous information systems research focusing on user information security behavior has established a gap in the literature and an absence of understanding. Threat severity, fear, and response costs were utilized by Posey et al. (2015) in their study on the effect of organizational dedication on insiders' security behavior. Posey et al. (2015) observed that threat severity, fear, and response costs became more significantly linked to protection motivation when the organizational dedication was at high levels, and not only in the conventional sense. Founded on this understanding, Posey et al. (2015) determined that the PMT constructs are valuable when utilized to give meaning to the cognitive, motivational, and past sequence of the behavior of users with high organizational commitment rather than low commitment.

Posey et al. (2015) used 380 insiders from several industries and positions within the United States. The study strived to investigate how company insiders may be motivated to maintain and enhance a company's information security. The study utilized portions of the PMT and depended upon unusual behaviors hence inhibiting the extrapolation of outcomes to specific items instead of a universal set of protective security behaviors. Posey et al. (2015) examined these motivations incapsulating a more behavioral set by assessing maladaptive enticements, response costs, and fear in conjunction with conventional PMT elements. Posey et al. (2015) extended PMT by revealing that: security education, training, and awareness (SETA) efforts assistance form appraisals, PMT's applicability to organizational rather than personal contexts depended on insiders' organizational commitment levels, and response costs provide the link between PMT's appraisals. Posey et al. (2015) posit that the company's dedication was vital in

the company's security threats mitigations, crucial personally to insiders, and how SETA efforts affect several PMT-based elements.

To further illuminate the reasons insiders act to protect their companies from information security threats, Posey et al. (2015) illustrated the often neglected factors linked to PMT like maladaptive rewards and response costs in the appraisal processes as they interact with protection motivated behaviors. Posey et al. (2015) have likewise shown how insiders' company's allegiance levels substantially moderate the processes stipulated by PMT; subsequently, the company's dedication is instrumental in shaping the company's information security threats relevant to insiders. Ultimately, organizational SETA attempts were proven to strengthen elements in both threat and coping appraisals, and SETA programs have been influential in persuading users to take security actions (Posey et al. 2015). Other user security mitigation studies were conducted in academic environments with students (Boss et al., 2015; Hanus & Wu, 2016)

Using 327 students, Boss et al. (2015) conducted two studies; the first one was a longitudinal study from the perspective of data backups, and the second a short-term cross-sectional study in the framework of anti-malware software. The study was aimed at information security (ISec) research to find ways to motivate people to participate in more secure behaviors. Boss et al. (2015) used PMT, which was regarded as a leading theoretical foundation in ISec research to assist in motivating people to alter their security-connected behaviors to protect themselves and their companies. Boss et al. (2015) reviewed the basis for PMT and found three prospects for enhancing ISec PMT research. These prospects mentioned present ISec studies not utilizing the complete nomology of PMT concepts; barely one study utilized fear-appeal strategies, a central component of PMT. Boss et al. (2015) specified the progress of studies in

forecasting security intentions but indicated that these studies never tackled actual security behaviors.

Furthermore, Boss et al. (2015) revealed how computer users demonstrated caution and engaged security-inclined behavior was similar in both the home and work environments and could be attributed to the persona rather than settings. Also, computer users employed security-minded behavior was ubiquitous in both the home and work environments (Boss et al., 2015). Boss et al. (2015) suggested that the approach of communicating secure practices is by Fear Appeals. The field of Information Security has a distinct demand to assess threats, vulnerabilities, and severity, as well as how the computer users would act in response to them since it was critical to understand how much fear to impart on each member of staff to counteract the threat (Boss et al., 2015). Boss et al. (2015) concluded that ISec PMT researchers ought to preferably employ and confirmed the core or complete nomology of PMT before combining non-PMT concepts and should preferably utilize fear-appeal strategies when carrying out security-connected PMT studies. Studies should measure fear when carrying out security linked PMT studies, and must correctly model and evaluate behaviors, not just intentions (Boss et al., 2015).

In another academic setting, Hanus and Wu (2016) conducted a three-week survey with 241 undergraduate college students. The goal of their study was to determine whether desktop security awareness influences desktop security behaviors from the PMT perspective. In their study investigating security behaviors in the home setting, Hanus and Wu (2016) found that two of the coping appraisal elements of PMT, self-efficacy, and response-efficacy were substantial predictors of specified security behavior. In contrast, the threat elements of perceived severity and perceived vulnerability did not predict secure behavior. They added to the literature by assessing the involvement of awareness, which is a valuable precursor to the cognitive practices

in the PMT. Hanus and Wu (2016) findings revealed that security awareness considerably alters perceived severity, response efficacy, self-efficacy, and response cost. Concepts in the coping appraisal process, in turn, substantially influence proposed security behavior (Hanus & Wu, 2016).

Hanus and Wu (2016) painted a clearer picture of how home users handle desktop security. The study also highlights how awareness should be thought of as a multidimensional concept by itself. The study outcomes also indicated that awareness of countermeasures was a critical determinant of coping appraisal processes. Therefore, it was simply not enough to be aware of threats if a person was not able to identify devices or methods that could help them implement protection. While this finding is against theoretical propositions of the PMT, previous PMT research has repeatedly shown that threat appraisal is a weak predictor of both behaviors and behavioral intentions. Hanus and Wu (2016) demonstrated that the two different dimensions of awareness were that of threats and countermeasures that had different influences on the behaviors of users. Hanus and Wu (2016) indicated that institutions could not merely instruct staff to be aware of security policies and practices. The study further emphasized user awareness training was an outcome of engagement via training leading to improved awareness of computer users, and users across the company must recognize security was each one's responsibility (Hanus & Wu, 2016). Usually, PMT-based behavior arose from a cognitive activity (Hanus & Wu, 2016)

Hanus and Wu (2016) concluded a complete understanding of the office antispyware software security without the comprehension of the behavior regarding spyware on their home computers. IS research focusing on home computing security behavior was limited (Hanus &

Wu, 2016), and was less about user security behavior in the home context compared to the business perspective.

Previous results obtained by Woon et al. (2005), Kumar et al. (2008), and Herath and Rao (2009b) have demonstrated that when the information security understanding and technical acumen of users type of business is low, perceived vulnerability does not substantially impact their security behavior. These results consequently imply that an individual's security experience performs a significant part in their perceptions of security about safeguarding from data compromise. Nevertheless, from a security viewpoint, variations in threats define real security function ultimately (Johnston & Warkentin, 2010).

Crossler and Bélanger (2014) adapted threat severity, threat vulnerability, and response costs in their study to build a unified security practices (USP) instrument. The growth of the USP was centered on the opinion that measuring multiple security behaviors rather than one better reflects the measures users need to take to safeguard their information assets. Crossler and Bélanger (2014) stated that perceived threat severity positively impacts the USP, while perceived threat vulnerability was unfavorable, and response cost had no significant relation with the USP. It is worth indicating that these outcomes were affected by the reliance of Crossler and Bélanger (2014) on actual behaviors for the USP and nontechnical individuals working in non-technically intensive fields as respondents.

Claar and Johnson (2012) used concepts that capitalized on embracing behavior based on severity and threat susceptibility. Antithetical to the results in the study by Crossler and Bélanger (2014), Claar and Johnson (2012) in a previous study discovered that threat severity did not have a substantial impact on user security behavior preceding to the threat occurring; instead, it was established as effective after the manifestation of the event. Likewise, Claar and Johnson (2012)

observed that threat vulnerability substantially affected user security behavior. The controlling variables of gender, age, education, and previous knowledge with security occurrences were utilized in the study to reach the conclusions. Claar and Johnson (2012) stated that fear had a major influence on behavior, and this was absent in previous security implementation paradigms.

The FAM established by Johnston and Warkentin (2010) in their study on Fear Appeals and information security behavior applied the PMT concepts of threat severity, threat vulnerability, and behavioral intent. According to Johnston and Warkentin (2010), the insertion of other aspects as a construct of FAM expanded earlier concepts and models like social influences (Thompson et al., 1991), image (Moore & Benbasat, 1991), and social norm that had been major in earlier study efforts at comprehending user behavior from the theory of reasoned action (Fishbein & Ajzen, 1975), and the theory of planned behavior (Venkatesh & Davis, 2000). Johnston and Warkentin (2010) used the expansion of FAM to emphasize the importance of behavioral intent, although they did proceed in testing actual usage, thus leaving a gap for future study. Furthermore, in prior research, the way web users can be further accountable for their security behavior on the Internet was examined, and the PMT constructs of threat severity and threat susceptibility were harnessed by LaRose et al. (2008) to create a framework for advocating secure cyber behavior.

Crossler et al. (2013) suggested that attempts to comprehend user information security behavior ought to contemplate behavior and change the emphasis of research from technical matters. Also, Kokolakis (2017) stated that there was a necessity for further study into the factors that can be exploited to impact the human element in information security and privacy. In the current literature, there is sufficient indication of the necessity for future study and a prospect for potential study based on the outcomes of the current study.

The Fear Appeals are a type of persuasive communication that usually inspires individuals to bring some change in their way of life, considering the potential risks that may occur due to their current way of life. In many ways, Fear Appeals have a background of successful outcomes (Komatsu et al., 2013; Ruiter et al., 2014; Yoon et al., 2012). For instance, the packaging of cigarettes has graphic warnings about the health risks that may come with smoking. First, this approach poses threats that occur to the life of the smoker, such as cancer. Second, a marketing campaign is launched to convey that smokers are more prone to developing cancers. Finally, the severity of the cancer is added to convey that smoking can be fatal (Ruiter et al., 2014).

Similarly, the risk of fatal accidents has been cited for drunk driving (Ruiter et al., 2014). Also, to help women in East Africa modify their lifestyles and encourage the early stage of breast cancer detection, fear appeals are used (Njoroge & Mberia, 2014). The idea behind PMT is also used in the healthcare field, just like Fear Appeals (Njoroge & Mberia, 2014; Boss, 2015; Yoon et al., 2012). Johnston and Warkentin (2010) suggested the use of Fear Appeals to encourage people to take protective measures during sexual activities to prevent HIV transmission.

The application of the Fear Appeals, with its roots in the field of healthcare, has been adopted in the world of information security (Yoon et al., 2012). At its root, the goal was to improve the behavior and responsiveness of computer users and make them understand that certain behaviors can be threatening. Awareness of the security activities and the implications of the risks connect PMT to the field of information security. The main benefit of PMT has been to influence a person's behavior and to motivate him/her to take specific actions to address the perceived risks.

There is a plethora of research about the general subject of fear appeals and the principle of security in residential settings. For example, McGill and Thompson (2017) examined the security differences between home computer users and mobile devices in the United States. Their research concentrated on the protection of mobile apps and raised concerns that home users do not read the safety messages, and even if they read them, they are mostly ignored. They found that the protection motivation of users was directed more to their computers and less towards safeguarding their mobile devices. They indicated that the users' age was a key factor.

Aurigemma et al. (2017) deliberated the opinions of home computer users in the U.S. regarding the use of password administration software. They noted that respondents felt that updating security systems for a home computer with the most recent security updates was voluntary and had a minimal impact, for example, malware or a ransomware attack. The authors suggested that the security behavior of the users of the home computers is restricted due to the lack of awareness of the risks, lack of knowledge of mitigating protection, and lack of voluntary willingness to act. In their report, Aurigemma and colleagues (2017) identified as much as eight factors organized into four categories, which motivated the study participants to use the similar password manager framework as recommended. The most common reasons for their participants' failure to download and use password administration software were individual factors like lack of time and lack of immediacy. The study established gullibility about threats or doubts regarding the possible security breaches caused by inadequate password administration (Aurigemma et al., 2017).

Menard et al. (2017) contrasted motives from the theories of self-determination and protective motivation. They analyzed the motivations of users when protecting their machines. Menard et al. (2017) did not exclude users of home computers, but their study did

relate to the current study since they did not differentiate between the home and office computer users. Menard et al. (2017) were of the view that although PMT was suitable for studying information system security, motivation was not examined as an aspect of the PMT model. Menard et al. (2017), therefore, have contrasted the factors based on the principle of the concept of self-determination and PMT.

In Fear Appeals communication (as measured by self-efficacy, response efficacy, and social influence), safety behavior of computer users is the area of significance, as found in Menard and colleague's research of 2017. Menard et al. (2017) found that embedded statements aimed at improving autonomy, competence, and safety appeal play a key role in improving the level of security. They demonstrated that motivation to respond to success significantly contributes to variation in a person's behavior. Based on the outcomes, the authors suggest that a future study should include a specific metric of motivation for one's own incentive to improve protective behaviors to protect his/her data (Menard et al., 2017). This result indicates the need for a study to be conducted in this area of research that should involve the motivational elements of communication of Fear Appeals, particularly when the actions of home computer users are modified or when the device defense systems are not adjusted per safety standards of their own personal computer.

The purpose of persuasive communication is to influence several gentle behavioral steps, which is called voluntary behavioral change (Taniguchi et al., 2014). Persuasive communication is used since workers are inspired to improve their work by obtaining new and valuable knowledge instead of financial rewards or constraints. People believe that the degree to which persuasive communication plays a role in achieving results has a tremendous impact (Taniguchi et al., 2014). Graton et al. (2015) discovered that guilt enhances the level of persuasive

compliance. Guilt only enhances compliance if the message has implications relating to the causes of guilt (Graton et al., 2015). A message is often used to modify behavior. The basic principle for persuasive communication, as noted by Hohman et al. (2015), is that social standards and behaviors were used to develop effective communication against tobacco use, which reduces uncertainty. Persuasive communication showed that people change their position on a subject with both positive and negative feelings based on mutual perceptions (Hohman et al., 2015).

For a more informative approach, Jenkins et al. (2014) focused on fear appeals using necessary organizational improvements, such as improvements in passwords. Jenkins et al. (2014), through PMT, addressed the issue of standard reuse of passwords. At the end of the study, 88.41% of employees used their default passwords to create new, strong, and unique passwords to reduce the threat of privacy invasion and data leaks (Jenkins et al., 2014).

Weakest Target in IS

Many kinds of weaknesses, vulnerabilities, and attacks can infiltrate a corporate network. Since it is appropriate to take home office work or to have people work remotely, a home computer user may access public Wi-Fi. In such scenarios, network protection needs to be considered to address the issues posed by the work-from-home concept (McGill & Thompson, 2017). No unique research on home computer users who infect corporate networks appears to be taking place.

Moreover, the general objective of network protection providers is to reduce vulnerabilities through strengthening a network's technical components like equipment, networking and software components, policies, culture, individuals, and internal processes (White et al., 2017; White, 2015). More than half of the entire data breaches are likely to result

from users obtaining unauthorized access to the network. Research evidence shows that events related to information security are growing. Such incidences can be minimized if companies concentrate more on the dangers posed by workers, especially those working from home (Bulgurcu et al., 2010; Guo et al., 2011; Shropshire et al., 2015; Spears & Barki, 2010). Therefore, corporate network security providers have the basis to be worried about the risks coming from the users of home computers.

User Security Noncompliance

Organizations develop policies regarding workplace standards to conform to security protocols. Such policies are targeted towards workers carrying out their assigned tasks using the organizational network. However, an understanding is emerging that policies need to be made to recognize work-at-home employees (Siponen et al., 2014). This awareness alone is not enough to address the broader cultural issue, which is that workers do not take proper security-related measures when they operate from home. Home users with access to confidential data worsen the issue further. While employees may wish to be compliant, they are still taken as the weakest link in protection against threats to the security of information (White et al., 2017). The explanation for the weakest link is that their adopted safety precautions are not in line with the requirements of the security protocols of the organizations (Shropshire et al., 2015).

The way people behave is highly risky and leads to a more severe problem. The risk maybe because of the passive non-compliance to organizational policies, unconscious behavior, and loss of motivation (Shropshire et al., 2015). There are also cases in which home computer users unintentionally take measures that are not in line with the corporate policy. This leads to increased risks to the security of the company's network (Guo et al., 2011). For example, unlicensed peer-to-peer file-sharing programs enabled to retrieve working files from home

computers tend to cause data leakage. Similarly, one can also pick weak/easily imagined passwords or just type the password in a sticky note and put it on the home screen in order to remember it (Guo et al., 2011; Siponen et al., 2014).

The fact that individuals are willing to pursue the right approaches, but they do not know the way to use the right methods, leads to a behavior-compliance discrepancy arising from several variables (Shropshire et al., 2015). About 24 percent of businesses say that their employees' non-malicious and irresponsible network usage was the cause of almost all their losses (Guo et al. 2011). McGill and Thompson (2017) supported and expanded this issue to users of home computers who operate from home. The research by Guo et al. (2011) split the actions of computer users into four categories for non-malicious safety violations, which include self-benefiting, intentional, free-will rule-breaking, and potential harm or security risk. There are several different motives for violating the rules. There are also variations between malicious, non-malicious, and unintentional behavior. Malicious behavior consists of the spreading of a virus, whereas non-malicious behavior may be a policy breach. A home computer user utilizing the home network is likely to perform actions that can risk both the office network as well as the home computer system.

The Social Influence in IS

Yu et al. (2013) identified the social impact on the perception of using a new system. This is apparent when the actions of an individual are changed based on the outside factors. The security perception regarding the use of the personal computer by a home computer user depends on the environment and social factors that influence the decision (Herath & Rao, 2009; Iftode & Pruna, 2014). Such factors include social impact if the actions of a group affect a person's behavior, minority impact if minority opinions affect majority behavior, systemic approach in

case of intergroup influences, and perspectives of the waiting states in case of external behaviors towards others (Iftode & Pruna, 2014).

Social factors can also affect the way people act in IT settings. Social impact studies have been carried out on how different factors influence the behavior of users of the IT services (Lin & Lu, 2015). The importance and purpose of using social influence as a factor is the reason it is explored in many technology-related studies. The study of social factors also plays a crucial role in recognizing the way people are motivated to act in their IT-related decisions (Jennings et al., 2015; Jennings et al., 2010; Li & Sakamoto, 2015).

Analysis of the Research Methods

The study intended to measure these constructs via convenience sampling to collect data from telecommuters who work with confidential data. The unit of analysis was the respondents, and the cross-sectional method was suitable since there was no requirement for the gathering of data at various moments in time. Furthermore, by analyzing the accumulated data, it was the objective to interpret the findings and draw inferences that was beneficial to the understanding of the security behavior of telecommuters.

From the earlier investigations, it was not evident that mixed research methods were extensively employed in information security behavior research. The use of the survey was the more common research approach in the previous studies examined. Posey et al. (2015), in their study on the influence of official dedication to insiders' security behavior, utilized a survey that was completed by 380 respondents. Crossler and Bélanger (2014) carried out a study to build on unified security practices (USP) instrument using web and paper-based survey with 324 respondents. In their study on security adoption behavior, Claar and Johnson (2012) employed a web survey to obtain data from 311 respondents. PMT model consisted of 547 responses.

Summary

The idea of Fear Appeals emerged in the healthcare industry, and, since then, it has been widely used to make people more mindful of their health. Health professionals usually make use of Fear Appeals by trying to scare people with potential repercussions. The Fear Appeals approach is now also being used in the IT industry with the intent to increase the security-consciousness of people by communicating to them the possible threats coming from non-compliance to the formal standards. The three Fear Appeals elements, as discussed in the paper, are threat, fear, and perceived efficacy.

Fear Appeals are a way of communicating with people the way to become more secure as well as the way to decrease the degree of computer usage associated risks. The 21st century stresses not only the use of technology but also its expansion. In 1975, with the goal of better recognizing the Fear Appeals and its perceived effects on people, Rogers (1983) developed the Protection Motivation Theory. This theory encompasses risks and threat management evaluation, where evaluation is based on self and response efficacy. It also encompasses threat appraisal that deals with severity and vulnerability related variables and their outcomes. The literature addressed in detail the security issues and threats that home computer users usually experience in various settings. It also deals with the corporate networks in several ways, for example, from the perspective of people bringing their office work to their homes, from the perspective of people doing office work within the office, and from the perspective of people dealing with financial, e-commerce, or healthcare-related services.

Chapter 3

Methodology

Overview of Research Methodology/Design

The research adopted a survey approach to evaluate how the independent variables – including self-efficacy, response efficacy, perceived threat severity, perceived threat susceptibility, and social influence - affect protection motivation, which, in turn, affects the dependent variable - security behavior of the telecommuters working with confidential data. This approach was utilized since it permitted quantitative data for statistical analysis to assess the hypotheses concerning the variables mentioned above. The study's approach is centered on a positivism philosophy since the data might support the hypotheses via the suitable utilization of theories and prototypes by prior researchers. Saunders et al. (2003) explained that a positivism approach would mean a very structured methodology so that another researcher can reproduce the study, and it also means the application of quantitative observations that permitted data to be analyzed statistically. When implemented, positivism philosophy delivers outcomes grounded on firmer arguments than sheer views or instinct (Burns, 2000). The broader view of the study targeted the security behavior of telecommuters from a data breach and spyware perspective. The study strived to determine a connection and envisage the influence amongst the concepts that have been put forward. The postpositivist philosophy was selected because the behaviors of computer users were studied. The significance was that the data stands for personal decisions and feelings contrary to being deeply rooted in a definite scientific fact. Post-positivism is, in many ways, the study of human nature and brought together theory and practice recognizing that many techniques can be used to collect the data (Hesse-Biber & Leavy, 2011).

Research Method

The main data gathering approach employed, was quantitative and involved using a survey. An online survey was devised for the objective of the current study. This data gathering method was selected due to its many advantages, rendering it suitable. Furthermore, views of many respondents were essential to collect highly consistent data without any unfairness; all the participants answered identical questions. The respondents took the survey whenever and wherever. Online surveys offered the benefit of procuring data proficiently in terms of period, activity, and expenditure. Online surveys made measurable data simpler to evaluate and understand, and also gathered normalized, computable data from a large sample size (Sekaran & Bougie, 2013).

SurveyMonkey administered the survey by sending out the link to the telecommuters via email. The sent email had a link that redirected the likely participants to the survey. The respondents reviewed a concise account of the research, informed consent, and confidentiality agreement. The survey and informed consent forms were uploaded to SurveyMonkey, and the respondents completed the online survey anonymously and unobserved. The survey was not in a typical environment with a negligible amount of meddling because measuring the chosen telecommuters was carried out in their natural settings.

The inclusion conditions were individuals who telecommute with access to confidential data, seek help when there was a problem with the computer and had anti-malware installed on the system. The respondents were adults of at least 18 years of age who reside in the United States and have access to confidential data over an organization's network. Those who did not meet the mentioned criteria were excluded. The research did not collect the identifying information of participants, and the data gathered for the study was kept confidential. Only the

researcher, dissertation mentor, dissertation committee, and Nova Southeastern University's IRB office could access the research data. Nova Southeastern University's IRB office approved the study before it was conducted and made public since it involved interaction with humans.

Instrument

The survey instrument for this research was a mixture of implementing and adjusting current scales. Saunders et al. (2003) proposed that employing or adapting existing scales was more effective than designing scales by oneself. The reason was that it helped in obtaining relevant data required to satisfy the study's demands. The survey was designed for easy comprehension in the most straightforward language, making it simpler for respondents to answer them.

The measurement standard for each of the following variables in the study objects was the interval scale. While the survey used the Likert scale, which was more oriented towards an ordinary measuring point, the actual measuring point for the analysis was viewed as an interval. The interval scale employment to evaluate individual survey variables warranted a simple quantification of the responses. This could also be conveniently evaluated with statistical methods. This measuring degree also meant the respondents were not pressured to adopt any perspective. Instead, it offered some amount of acceptance, dissension, or even indifference and uncertainty.

The study utilized a 7-point rating scale on all survey objects. The instrument's reliability was checked because it is critical to base this analysis on accurate and impartial data. The Cronbach alpha test for reliability of the items was therefore performed. Gay et al. (2009) recommended Cronbach's alpha as a better way to determine internal accuracy when a research survey system uses the Likert scale. If the different variables return a value of 0.7 or higher

Cronbach's alpha, the result of the process is of reasonable reliance. A value of no less than 0.7 for Cronbach's alpha core should be attained since it is the lower limit intended for reliability in validating research.

The constructs included response efficacy (RESP), self-efficacy (SEFF), threat severity (TSEV), social influence (SINF), and threat susceptibility (TSUS). The constructs were multi-item scales taken from earlier validated measures adapted to relate precisely to security responses to computer viruses and malware. SINF was tailored from Johnston and Warkentin (2010), while SEFF, TSUS, and TSEV, and BHAV were constructed from Johnston and Warkentin (2010), Claar and Johnson (2012), and RESP from Boss et al. (2015) and Johnston and Warkentin (2010). The items were evaluated using a seven-point Likert scale. The protection motivation questions (PM) were derived from Posey et al. (2015), and computer security usage (CSU) was adapted from Claar and Johnson (2012).

The items for measuring perceived threat severity and perceived threat susceptibility were adapted from Claar and Johnson (2012) and Johnston and Warkentin (2010). The items for the two constructs evaluated the degree to which people feel that it is likely that they would experience a scenario and evaluated the effect on them when it occurred (Boss, 2007). The items for perceived threat severity were measured on a 7-point Likert scale ranging from "1" = Very Low Impact to "7" = Very High Impact. The items for perceived threat susceptibility were measured on a 7-point Likert scale ranging from "1" = Highly Unlikely to "7" = Highly Likely. The reliability test for the adapted items had a Cronbach's alpha of 0.91 for perceived threat severity and 0.92 for perceived threat susceptibility (Claar & Johnson, 2012). A scale was adapted from Johnston and Warkentin (2010) to measure social influence. The items for social influence were measured on a 7-point Likert scale ranging from "1" = Strongly Disagree to "7" =

Strongly Agree. The reliability measured for the adapted items had a 0.84 Cronbach's alpha (Johnston & Warkentin, 2010).

The response efficacy scale was adapted from Boss et al. (2015) and Johnston and Warkentin (2010). The reliability of the modified items assessed was Cronbach's alpha of 0.89 (Boss et al., 2015; Johnston & Warkentin, 2010). The items for response efficacy were evaluated on a 7-point Likert scale ranging from "1" = Strongly Disagree to "7" = Strongly Agree. To measure computer self-efficacy, a scale was adapted from Claar and Johnson (2012). Computer self-efficacy items were measured on a 7-point Likert scale ranging from "1" = Strongly Disagree to "7" = Strongly Agree. The reliability of the adapted items was a Cronbach's alpha of 0.94 (Claar & Johnson, 2012).

The items for protection motivation were adapted from Posey et al. (2015). The items for protection motivation were measured on a 7-point Likert scale ranging from "1" = Strongly Disagree to "7" = Strongly Agree. The reliability of the adapted items was a Cronbach's alpha of 0.64. Posey et al. (2015) pointed out that an alpha below 0.70 for protection motivation agrees with the needs from past studies, and a lower alpha was usually the case when an instrument had fewer items. Computer security usage was measured by adapting a scale from Claar and Johnson (2012) and self-developed items. Computer security usage items were measured on a 7-point Likert scale ranging from "1" = Never to "7" = Always. The reliability of the adapted items was 0.90 Cronbach's alpha (Claar & Johnson, 2012).

The survey that was carried out was extremely relevant in resolving the hypotheses since it offered crucial information on the variables that were established in the hypotheses. The reliability and validity of the item's constructs were essential (Straub, 1989). The items used for each construct could be found in Table 1.

Table 1

Constructs Items and Instrument Source

Constructs/Items	Description	Source
Perceived Threat Severity	Please indicate the impact that each of these scenarios would have on you if it would occur.	
TSEV1	My computer was infected by spyware.	Johnston and Warkentin (2010)
TSEV2	My computer is becoming corrupted by a virus.	Claar and Johnson (2012)
TSEV3	My computer being taken over by a hacker.	Claar and Johnson (2012)
TSEV4	Sensitive data being stolen from my computer.	Claar and Johnson (2012)
TSEV5	Sensitive data being lost due to a virus on my computer.	Claar and Johnson (2012)
TSEV6	My computer is downloading a virus or an application with many bugs.	Claar and Johnson (2012)
Perceived Threat Susceptibility	Please indicate how likely you feel each scenario will occur with your computer.	
TSUS1	My computer is at risk of becoming infected with spyware.	Johnston and Warkentin (2010)
TSUS2	My computer will likely become infected with spyware.	Johnston and Warkentin (2010)
TSUS3	My computer may become infected with spyware.	Johnston and Warkentin (2010)
TSUS4	My computer becoming corrupted by a virus.	Claar and Johnson (2012)
TSUS5	My computer being taken over by a hacker.	Claar and Johnson (2012)
TSUS6	Sensitive or confidential data being stolen from my computer.	Claar and Johnson (2012)
TSUS7	Sensitive or confidential data is lost due to a virus on my computer.	Claar and Johnson (2012)
TSUS8	My computer is downloading a virus or an application with many bugs.	Claar and Johnson (2012)

Self-Efficacy	Please indicate the degree to which you agree or disagree with the following statements.	
SEFF1	Using anti-spyware software increases my productivity.	Johnston and Warkentin (2010)
SEFF2	I am confident about selecting the appropriate security software on my computer.	Claar and Johnson (2012)
SEFF3	I am confident about selecting the appropriate security settings on my computer.	Claar and Johnson (2012)
SEFF4	I am confident of correctly installing security software on my computer.	Claar and Johnson (2012)
SEFF5	I am confident of quickly finding information on using security software on my computer.	Claar and Johnson (2012)
Response Efficacy	Please indicate the degree to which you agree or disagree with the following statements.	
RESP1	Using anti-virus software works to protect my computer from a data breach	Boss et al. (2015); Woon et al. (2005)
RESP2	Using anti-malware software works to protect my computer from a data breach.	Boss et al. (2015); Johnston and Warkentin (2010)
RESP3	Using anti-virus software is effective in protecting my computer from a data breach.	Boss et al. (2015); Johnston and Warkentin (2010)
RESP4	Using anti-malware software is sufficient to protect my computer from a data breach.	Boss et al. (2015); Johnston and Warkentin (2010)
RESP5	Using anti-virus software would more likely protect my computer from a data breach.	Boss et al. (2015); Johnston and Warkentin (2010)
RESP6	Using anti-malware software would more likely protect my computer from a data breach.	Boss et al. (2015); Johnston and Warkentin (2010)

RESP7	Installation and frequent updates of anti-virus software is effective in preventing virus infections on my computer	Hanus and Wu (2016)
RESP8	If I install anti-virus software on my computer and update it frequently, I am less likely to have my system infected by a virus	Hanus and Wu (2016)
Performance Expectancy	Please indicate the degree to which you agree or disagree with the following statements	
PERF1	I find the use of anti-spyware software useful in my job.	Johnston and Warkentin (2010)
PERF2	Using anti-spyware software enables me to accomplish tasks more quickly.	Johnston and Warkentin (2010)
Social Influence	Please indicate the degree to which you agree or disagree with the following statements	
SINF1	People who influence my behavior think that I should use anti-spyware software.	Johnston and Warkentin (2010)
SINF2	In general, my organization has supported using and providing anti-spyware software.	Johnston and Warkentin (2010)
Attitude	Please indicate the degree to which you agree or disagree with the following statements	
ATT1	Anti-spyware software makes work more interesting.	Johnston and Warkentin (2010)
ATT2	Working with anti-spyware software is fun.	Johnston and Warkentin (2010)
ATT3	I like working with anti-spyware software.	Johnston and Warkentin (2010)
ATT4	Working with anti-spyware software is enjoyable.	Johnston and Warkentin (2010)
Protection motivation	Please indicate the degree to which you agree or disagree with the following statements.	
PM1	I am motivated to protect my computer from threats of a data breach.	Posey et al. (2015)

PM2	I am motivated to prevent threats of a data breach to my computer from being successful	Posey et al. (2015)
PM3	I am motivated to engage in activities that protect my computer from threats of a data breach.	Posey et al. (2015)
Computer Security Usage	Please indicate the frequency you perform the following tasks	
CSU1	I use firewall protection on my computer.	Claar and Johnson (2012)
CSU2	I use anti-virus software on my computer.	Claar and Johnson (2012)
CSU3	I use anti-malware software on my computer.	Claar and Johnson (2012)

All the instruments were previously validated (Claar & Johnson, 2012; Claar, 2011; Boss et al., 2015; Hanus & Wu, 2016; Johnston & Warkentin, 2010; Posey et al., 2015; Woon et al., 2005), hence, did not need reliability test. The quality of an instrument was paramount since it evaluated the variables accurately and determined the integrity of the measures. The research conducted a series of preliminary analysis to guarantee the quality of the instrument consisting of reliability and validity. The content validity was crucial to eliminate constructs from formative scales established on theoretical approaches that weakened the strength of the instrument (Diamantopoulos & Winklhofer, 2001). Construct validity defines the extent to which every single measure accurately determines its targeted variable.

This survey was designed to investigate telecommuters to mitigate threats with the suggested course of action when a threat is encountered. The survey was made up of Likert-type questions and categorical demographic questions. The instrument established a specific scoring of information. However, composite scores were created for each of the survey sub-sections by creating a mean score from the relevant survey items. The Likert-style rating scale, to be precise, was a 7-point rating scale on all survey items. The instrument's reliability was tested because the

current study was based on reliable data that was more objective. Therefore, the Cronbach alpha test was performed to assess the reliability of the items. Rovai et al. (2013) further explained that a factor loading below 0.5 is regarded as a low Cronbach's alpha coefficient. The average for a coefficient between 0.5 and 0.7, and above 0.7 is considered high.

While a survey instrument itself may increase a participant's intention of performing a specific information security behavior, this might not be the survey instrument's objective; meanwhile, the spotlight is usually on realizing the connection between some constructs and a person's current behavior (Dupuis, 2016). Therefore, self-reports of behavior was measured in the current study, which was considered an essential step towards measuring actual behavior. The usage of self-reports to assess security-related behavior could lack validity since self-reports are predisposed to the challenges of standard method variance, consistency theme, social suitability, and the outcomes might be subjective (Siponen, 2000). Workman (2008) indicated that self-reports might not be enough prognosticators of the actual behavior of computer users, since the self-reported opinions of security behavior of computer users are sometimes not intended to align with their actual security behavior.

Ethical Consideration

The IRB at Nova Southeastern University was engaged for consent to carry out the study. The IRB needs and requirements for the gathering and managing information were observed for the study's objective. The respondents were introduced to the purpose of the survey and that their contribution was optional; the data was kept private and only employed for the study. Respondent information was handled with rigorous confidentiality. SurveyMonkey utilizes strongly encrypted servers and reassures its users that all data is maintained secure and confidential. Ethical problems in the construction of the survey were averted, and the insertion of

items that pursued personal data such as name and job title could deter respondents from partaking because sustaining their privacy may not be guaranteed. Respondents had insignificant threats and were utterly voluntary. An informed consent form describing the study's nature, what was involved, and the voluntary aspect of participation was offered. The entire data was kept on protected hard drives with access just by the researcher.

Population and Sample

The population was comprised of telecommuters in the United States, working with confidential data via their organization's network. Non-probabilistic sampling was used since it targets a population. These were adults working from home for a company while accessing sensitive or confidential data. The population included respondents with varied educational backgrounds, age, and other demographic factors. The intent of targeting this population was to determine how people working in a home setting reacted to threats when they were in a situation that they were not obliged to respond in a certain way to that threat.

The current study was conducted using a wide variety of respondents across the United States in the comfort of their home settings working with sensitive data to see if there was a relationship between self-efficacy, response efficacy, threat severity, perceived threat severity, perceived threat susceptibility, and social influence on the security behavior of telecommuters. Since security behaviors are the dependent variable and a vital feature of the study, there was no differentiation between the education of the participants or work industry, except that they had access to and worked with sensitive data while telecommuting. Security was very crucial to the respondents since they access confidential information.

When considering the sampling of those telecommuters working from home with access to confidential data, there was no need to ascertain the sample size for a proportion. The current

study strived to determine the extension to the general population via a dependable and acceptable sample size, including accuracy with a margin of error of $\pm 5\%$, a standard deviation of 0.5, and a confidence level of 95%. The estimated population was 1053, which included users working from home with access to confidential data and have an antivirus installed on their computers.

The survey company collected all the data, using a population of 1053 persons, and 926 responded, but was filtered to only those who worked from home with confidential data and have anti-virus software installed on their computers, subsequently narrowing to a final count of 376 for analysis. The response rate could not be conveniently determined since the data was collected and filtered. The 376 individuals used for analysis was very reasonable, 36% of the 1053 surveys sent out originally. According to Sekaran and Bougie (2013), the response rate should be at least 30%. Even a 30% response rate is deemed adequate and outstanding in several situations (Sekaran & Bougie, 2013). Johnston and Warkentin (2010), in their groundbreaking study launching the FAM, attained a reply rate of 40% employing an online survey that was devoid of incentives. Also, no incentives were offered to the respondents in the current study. Email notices were sent to SurveyMonkey participants to improve the response rate. IRB approval was attained before the recruitment of subjects.

Power Analysis

Experimental models that encompass progressively rigorous methods for various factors pose their own set of challenges, such as acquiring a large enough sample size to provide sufficient statistical power (Cohen, 1988; Price et al., 2005). As significant as they may be, the presence of such challenges does not alleviate the need for more significant consideration to be given to such approaches. G*Power version 3.1.9.7 provided improved effect-size calculators

and graphic options since it encourages the distribution-based and design-based input methods and offers all types of power analyses in which users might be interested (Faul et al., 2007). G*Power software was a useful power analysis tool for various statistical tests despite not providing a thorough demonstration of needed sample sizes (Faul et al., 2007). Effect-size indexes and conventional values are given for operationally defined small, medium, and large effects (Cohen, 1992). Howell (2010) recommended that to determine sample size, the power level ought to be close to 0.8, alongside an alpha of 0.05, and as a minimum, a minute effect size. Appropriately, G*Power 3.1.9.7 was utilized to evaluate the sample size employing a power of 0.8, an alpha of 0.05, and a medium effect size (f^2) of 0.15 (Cohen, 1992). When these variables were used, the sample size was 270. This implies the 376 size was about 39% more than anticipated.

Pre-analysis Data Screening

The dataset was downloaded from SurveyMonkey into SPSS for data management and analysis. The data were screened for accuracy, missing information, and outliers tested by checking the standardized values. Standardized values denote the number of standard deviations of the mean value. Deviations higher than 3.29 and less than -3.29 standard deviations from the mean were considered outliers (Altman & Bland, 2005). Participants who did not finish the essential sections of the survey were excluded. Compound scores that signified the variables used were created by calculating an average score on each survey's subscales. Descriptive statistics describe the sample demographics and the research variables used in the analysis. Howell (2009) stated that percentages and frequencies were determined for categorical data, whereas averages and standard deviations were calculated for continuous data.

Data Analysis Strategy

The Partial Least Squares Methodology to Structural Equation Modeling (PLS-SEM) via Smart PLS 3.2.7 to evaluate the research model was used (Byrne, 2001). PLS-SEM was suitable mainly for studies focused on prediction where the aim was to describe the variance observed in the dependent variable, as with this research, which was focused on understanding protection motivation (Byrne, 2001). This approach is also suitable when many constructs are included in the research model, with the model being relatively complicated compared to the sample size (Hair et al., 2011).

The justification of the PLS-SEM for the objectives was highlighted by Byrne (2001), indicating that it was a useful statistical technique when carrying out a study with underlying associations. Hair et al. (2011) recommended that when Covariance Based Structural Equation Modeling (CB-SEM) contrasts with PLS-SEM, the latter was more effective in situations with prediction-oriented objectives. PLS-SEM was more amenable with sample sizes and handled the problem if concepts were formative or reflective. The data's conception utilized scatter plots and other graphs to summarily provide the review done to portray the asymmetrical constructions and modification (Mertler & Vannatta, 2013).

Presenting the Results

The research outcomes were presented in a format that made it effortless for the reader to understand. The data gathered from the survey was evaluated and shown in the current study report. The PLS-SEM and SPSS tools were used to generate figures, outputs for data analysis were displayed in the report results section, and the screenshots were in the appendices. The necessary validity test outcomes, such as the Cronbach's alpha was displayed in tables for simplification purposes. The survey template used to collect data was displayed in the

appendices and the approved IRB. The Nova Southeastern University Dissertation Guide for the College of Computing and Engineering Doctoral for students was used to discuss the research report.

Resource Requirements

Resources needed included, peer-reviewed journals, laptops, books, and reliable literature to assist the study. The relevant literature and information for the study were mostly from the Alvin Sherman Library of Nova Southeastern University. Also, SurveyMonkey was utilized to administer the survey questionnaire and data collection. The study involved human subjects in doing surveys and consequently obtained IRB approval before the data were collected. Smart PLS 3.0 and SPSS were employed for data analysis, interpretation, and presentation of the outcomes in any suitable format.

Summary

A quantitative methodology design was employed. The target population was a telecommuter working with sensitive data over the age of 18, living in the United States. Concerns of generalizability were assessed by comparing the sample's demographic characteristics and the population. The link among self-efficacy, response efficacy, threat severity, perceived threat severity, perceived threat susceptibility, and social influence was established. The sampling strategy was quantitative research.

A survey was employed to determine correlations and connections between constructs. Ensuring validity and reliability in the research is essential. The sampling type was convenience sampling since the current study gathered data from a group of telecommuters working with confidential data. The data analysis plan included the use of SPSS and PLS-SEM. The results were presented in the related sections and the appendices with assistance from the Nova

Southeastern University Dissertation Guide for the College of Computing and Engineering for doctoral students. The needed resources were obtained and available for the study.

Chapter 4

Results

Data Screening

After IRB approval was obtained, the web-based survey was administered via SurveyMonkey (see Appendix A). The cross-sectional method was leveraged to collect data during October and November 2020. The survey company collected all the data, with about 1053 persons who responded. The demographic information was collected by SurveyMonkey using census data to reflect the population in the United States of America. According to SurveyMonkey, out of all the respondents, 926 (response rate of 88%) completed the survey questions, but 130 (12%) of the respondents abandoned the survey. Most participants (89%) had more than three years of experience with a computer, while only 2% said they had less than six months. This sampling shows that the respondents were mostly computer literate based on their experience and education level. The data were filtered to extract those who work from home with confidential data and have anti-virus software installed on their computers, resulting in a final count of 376 for analysis.

The respondents were broken down as follows: 51% were female and 49% male. The age varied substantially as indicated: 18 to 29 (25%), 30 to 44 (29%), 45 to 60 (32%), and over 60 (14%) (see Appendix B). Most of the respondents had a bachelor's degree (40 %) though the level of education ranged from high school completion (11%) to doctorate (3%). Most (93%) had read or heard about security breaches, and for 65% of the respondents, their computer had been affected by a security breach (e.g., malware, virus). The final dataset consisted of 368 participants after dropping eight outliers from the original 376 participants. The Skewness and Kurtosis of the data before deleting the outliers were 3.602 and 25.392, respectively (see

Appendix C). The Skewness and Kurtosis values dropped to 1.090 and 0.997 (see Appendix D). The Skewness and Kurtosis conform to Hair et al. (2017) recommendations for accepting a normal distribution from -1 to +1. The sample size was about 36% higher than the statistically calculated sample size using G*Power 3.1.9.

The act of protecting a device from spyware and computer security behaviors were considered as they would apply to a standard home computer like a desktop or a laptop and the utilization of remote devices (phones or tablets). While the study was focused on home computer users, security behaviors are not just measured for laptops and desktops; they also include tablets and phones. Established on the U.S. Census Bureau (2015), the population entailed roughly equal amounts of men and women. Hence, the sample was representative of the general population. The population consists of roughly 30% Baby-Boomers (U.S. Census Bureau, 2015), which is marginally less than the percentage found in the sample. The population consisted of 70% of individuals with three or more years working with a computer, analogous to the sample percentage (Fil & Ryan, 2014).

The pre-analysis of data determines the nature and extent of biases attributable to missing data (Hensher, 1987). The paper discusses various ways of correcting for identified bias. The methods outlined are separated into those statistical procedures suitable for testing and correcting at the aggregate level. Petersen and Ekstrøm (2019) indicated data scrubbing and validation in the pre-data analysis are essential steps in every data analysis, while the validity of the conclusions from the assessment hangs on the quality of the survey data. Inaccuracies in the data can occur due to inaccurate codings and faulty survey instruments (Petersen & Ekstrøm, 2019). Data visualization methods in the pre-data analysis were not limited to graphs; scatter plots and

screen plots were employed to concisely present the analysis performed to illustrate unusual structures and discrepancies (Mertler & Vannatta, 2013).

Mahalanobis Distance and Box Plot

The Mahalanobis distance was utilized to recognize and eradicate multivariate outliers. The data were assessed for multivariate outliers using a Mahalanobis Distance Test (Tabachnick & Fidell, 2013). Eight multivariate outliers were identified and removed using SPSS. The chi-square's critical value at $p < .001$ was used to calculate the Mahalanobis distance. According to Mertler and Reinhart (2017), the agreed criterion for outliers is a value for Mahalanobis distance significance beyond $p < .001$, determined by assessing the acquired value for Mahalanobis distance to the chi-square critical value. Eight of the responses were removed due to their p values less than .001. The Mahalanobis distance was recalculated (see Appendix D) after the removal. Mertler and Reinhart (2017) pointed out that outliers should not be automatically dropped from the analysis since they may be unusual cases, but totally legitimate, rather than considered flawed. After recalculating the Mahalanobis distance with 368 cases, two outliers were realized but not dropped after as supported by the normality and scatter plots (see Appendix D).

Normality and Scatter Plot

The study variables were grouped into independent and dependent variables for a normality test. As evident in the box plot, the Skewness and Kurtosis of the data before deleting eight of the most extreme outliers, the Skewness and Kurtosis were 3.602 and 25.392, respectively (see Appendix D). The Skewness and Kurtosis values dropped to 1.090 and 0.997 (see Appendix D), following the deletion of the eight extreme outliers. After analyzing the normality test, the eight deleted extreme cases showed normal distribution according to the plots.

Hair et al. (2017) suggested accepting a normal distribution when its skewness and kurtosis range from -1 to +1. The statistical choices, data conception, and graphical techniques may not be restricted to Skewness and Kurtosis only (Mertler & Reinhart, 2017). The Kolmogorov-Smirnov statistic plus Lilliefors significance level, ANOVA, histogram, normal P-P plot of regression, and scatter plots ought to be utilized to check data for normality, linearity, and variance. The data distribution was normal, as depicted by the statistical outputs and normality graphs (see Appendix D). The cases were roughly on the diagonal line for both the normality Q-Q and normality P-P regression plots. The scatter plot likewise created a rectangular shape, which revealed a virtually normal distribution (see Appendix D).

Data Analysis

The structural models were analyzed using structural equation modeling. The software used for analysis was SmartPLS version 3.0 (Ringle et al., 2005). SmartPLS is a component-based (partial least squares) structural equation modeling tool that is both easy to use and free for academic use. The PLS approach to structural equation modeling was considered particularly appropriate for the study due to the multiple dimensions, formative constructs, and general theory-building that is taking place (Hair et al., 2011; Jenkins et al., 2014). The analysis entailed examining the model weights and evaluating the R^2 values for the latent constructs (Petter et al., 2007). Given that the instruments were developed with having formative first-order and formative second-order constructs, it was vital to analyze them using appropriate techniques since there was no direct approach to evaluate dimensions in partial least squares applications.

The approach utilized was in accordance with Ringle et al. (2015). However, incorporating these other components allowed for analysis of each of these instruments, including path coefficients, R^2 scores, and tests for significance (i.e., t-statistic) information. All

PLS analyses that were conducted included the following settings: use of mean replacement for missing values, path weighting scheme as the weighting design, and initial weights of 1.0. Likewise, calculations for significance testing utilized the bootstrapping technique with the mean replacement for missing values and 500 subsamples.

Bootstrapping requires "resampling" the data with substitution several times to create an empirical estimate of the whole sampling distribution of a statistic (Hox et al., 2017). The bootstrapping method is an exceedingly beneficial option compared to the conventional approach of hypothesis testing since it is relatively uncomplicated, and it mitigates several pitfalls of the conventional method (Preacher & Hayes, 2004). Statistical inference usually depends on the sampling distribution and the standard error of the characteristic of concern. The conventional method or huge sample method draws one sample of size from the population, and that sample is employed to determine the population approximations to create inferences (Hox et al., 2017). Bootstrapping is a better approach when the sample size is relatively small and also when the population is unknown, as is the case in this study. The bootstrapping procedures are very thorough in that they present users to use various confidence interval types, choose between one- and two-tailed testing, and stipulate significance levels (Sarstedt & Mooi, 2019). Since this was mostly exploratory research with hypothesized relationships, significance levels were provided at the $\alpha=0.10$, $\alpha=0.05$, and $\alpha=0.01$ levels, one-tailed.

Data analysis was achieved utilizing the Smart PLS 3.0 tool. The tests carried out comprised model fit, factor loading, construct reliability and validity, outer loading, discriminant validity, path coefficients, and bootstrapping. The PLS algorithm was executed, and all the factor loadings agreed with the acceptable value of 0.70 except SEFF_1 (see Appendix E).

Instrument Reliability and Validity

According to more analysis of the construct reliability and validity output, the average variance extracted (AVE) was deemed reliable as they met the accepted value of 0.5 or higher (see Appendix F). Nonetheless, the constructs utilized had Cronbach's alpha and composite reliability ranging from 0.7 to 1.0, except for the social influence (0.681); therefore, indicating reliability. The reliability processing results were assessed to have a valid significant level of reliability if the individual variables each have a Cronbach's alpha of 0.7 or more (Gray et al., 2009). Rovai et al. (2013) also indicated that a value of 0.70 at a minimum must be attained as it is the lower limit for Cronbach's alpha internal consistency reliability in confirmatory research. Each of the AVE was very good and beyond the 0.5 recognized value. It was devoid of deleted items in the construct. The Cronbach's alpha, composite reliability, and AVE's outcomes indicated that the measurement items employed demonstrated convergent validity. The Cronbach's alpha of 0.681 for the Social Influence had only two items in the construct, and it is often the case with limited items to get lower alpha values. The overall Cronbach's alpha of the entire instrument was 0.817, hence achieving a value greater than the required 0.70 (see Table 2; Appendix G; Appendix H).

The model fit was evaluated after running the PLS algorithm. According to Hu and Bentler (1998), and SRMR value below 0.08 signifies a good fit when utilized in CB-SEM. Hair et al. (2012) indicated that the definite statistical theories of the CBSEM and PLS-SEM foster an added compliment, as the fragility of one, is the strength of the other.

Table 2

Instrument Reliability and Validity

	Cronbach's		Composite	Average Variance
	Alpha	rho_A	Reliability	Extracted (AVE)
Computer Security Usage	0.903	0.904	0.903	0.757
Perceived Threat Severity	0.951	0.955	0.951	0.764
Perceived Threat Susceptibility	0.961	0.962	0.96	0.750
Protection Motivation	0.902	0.903	0.902	0.754
Response Efficacy	0.932	0.937	0.93	0.628
Self-Efficacy	0.877	0.879	0.879	0.591
Social Influence	0.681	0.743	0.704	0.551

The SRMR for the model fit was 0.053 and below the 0.080 value, signifying a good fit (Hair et al., 2017) (see Table 3; Appendix H). Hair et al. (2017) termed the model fit's SRMR in the same way as a standardized root means square residual.

Table 3

Model Fit and Accepted Values

	Saturated Model	Estimated Model
SRMR	0.053	0.168
d_ ULS	1.761	17.851
d_ G	1.060	1.430
Chi-Square	2110.886	2643.838
NFI	0.829	0.786

Convergent Validity

One possible validation approach is to assess patterns of correlation between items and constructs (Petter et al. 2007). Diamantopoulos and Winklhofer (2001) propose that formative items correlate with a universal item that summarizes the construct's essential nature. PLS item weights, which signify the influence of discrete formative items (Bollen & Lennox, 1991), can be multiplied by item values and tallied (Bagozzi & Fornell, 1982). Essentially, these outcomes in an altered multitrait, multimethod (MTMM) matrix of item-to-construct, and inter-item correlations akin to that evaluated by Bagozzi and Fornell (1982) and Loch et al. (2003). The consequent matrix displays item-to-construct correlations (Table 4; Appendix H).

Table 4

Inter-Item Correlations Matrix

	TSEV	TSUS	SEFF	RESP	PERF	SINF	ATT	PM	CSU
TSEV	1.000	0.132	0.278	0.343	0.191	0.337	-0.081	0.415	0.436
TSUS	0.132	1.000	0.062	0.029	0.164	0.093	0.339	-0.084	-0.078
SEFF	0.278	0.062	1.000	0.605	0.497	0.500	0.401	0.493	0.523
RESP	0.343	0.029	0.605	1.000	0.569	0.646	0.338	0.614	0.682
PERF	0.191	0.164	0.497	0.569	1.000	0.515	0.522	0.411	0.421
SINF	0.337	0.093	0.500	0.646	0.515	1.000	0.378	0.567	0.590
ATT	-0.081	0.339	0.401	0.338	0.522	0.378	1.000	0.178	0.094
PM	0.415	-0.084	0.493	0.614	0.411	0.567	0.178	1.000	0.778
CSU	0.436	-0.078	0.523	0.682	0.421	0.590	0.094	0.778	1.000

Following Campbell and Fiske (1959), Loch et al. (2003) proposed that convergent validity is displayed if items of the same construct correlate significantly with their corresponding composite construct value (item-to-construct correlation). This requirement has been fulfilled, as all items correlated significantly ($p < 0.01$) with their respective construct

composite value. Therefore, the results indicated an acceptable level of convergent validity of 0.5. Discriminant validity can be established if item-to-construct correlations are higher with each other than with other construct measures and their composite values (Loch et al. 2003). This condition was also met. Construct validity tests were also conducted for reflective variables. Factor loadings were examined to ensure that items loaded on intended constructs did not cross-load on constructs to which they should not load (Straub et al. 2004). Generally, convergent validity is demonstrated if the item loadings are more than 0.70 on their respective factors, and the average variance obtained (AVE) for every construct is above 0.50 (Gefen & Straub, 2005).

Discriminant Validity

The discriminant validity was evaluated using the Fornell-Larcker criterion; the diagonal value must be greater than the row and column values. The AVE's square root for the construct was more than the inter-construct correlation. The discriminant validity was also assessed by heterotrait-monotrait (HTMT) ratio of correlations (Henseler et al., 2015), with values lower than the threshold of 0.90. Therefore, discriminant validity was attained. The discriminant validity guarantees that a constructed measure is analytically distinctive and signifies phenomena of importance that other methods in a structural equation model do not portray (Henseler et al., 2015).

Chin (1998) recommended that all variable's loading to itself must be higher in value contrasted to its cross-loadings with other variables to ascertain discriminant validity. Fornell and Larcker (1981) described discriminant validity as established once the latent variable has a greater variance in its related variables contrasted to its values when cross-loaded with other constructs in the identical model. The discriminant validity test outcomes revealed that the

diagonal loadings are more than each of their cross-loadings and ranged from 0.860 to 0.912.

Discriminant validity is thus profound in measuring the items (see Table 5; Appendix H).

For discriminant validity, the results also showed the square root of the AVE values (shown on the diagonals), as indicated earlier in the chapter, was greater than the correlations among the constructs, signifying that the constructs were distinct from each other (Hair et al., 2014).

Table 5

Discriminant Validity

	Computer Security Usage	Perceived Threat Severity	Perceived Threat Susceptibility	Protection motivation	Response Efficacy	Self- Efficacy	Social Influence
Computer	0.912						
Security Usage							
Perceived Threat	0.450	0.894					
Severity							
Perceived Threat	-0.070	0.113	0.882				
Susceptibility							
Protection	0.821	0.444	-0.101	0.908			
motivation							
Response	0.727	0.323	0.034	0.704	0.811		
Efficacy							
Self-Efficacy	0.553	0.297	0.056	0.526	0.620	0.824	
Social Influence	0.613	0.339	0.078	0.642	0.690	0.516	0.860

For the structural model, attention is paid to the R^2 values (i.e., coefficient of determination) and path coefficients (Hair et al., 2014). The R^2 value signals how great the model's fit was; the

higher the R^2 value, the greater the fit, and the better the model represented the data collected (Chin, 1998). The outcomes (see Appendix H) showed an R^2 value of 0.672, suggesting the model portrayed a moderate to a substantial proportion of the variance observed for protection motivation (see Appendix H).

Findings

The hypotheses were tested using the Smart PLS 3.0 tool. Bootstrapping with a 500 resampling was done to assess the significance of the research model's paths as presented earlier. The bootstrapping execution generated a t -statistic (t -values) that illustrated the significance of the structural path. According to Hair et al. (1995), the level of significance is for a t -value exceeding or equal to 1.96 was deemed significant and adequate for research values using a two-tailed test with a 5% significance level. Hair et al (2011) indicated that the specific path coefficients of the PLS fundamental pattern can be adopted as standardized beta coefficients (β) of ordinary least squares regressions. The beta coefficient related the strength of the impact of the independent variable to a corresponding dependent variable; the greater the absolute value of the beta coefficient, the greater the impact (Hair et al, 2011).

The independent constructs showed variance on the dependent construct with protection motivation, 55 percent explained by response efficacy, self-efficacy, and social influence. The independent constructs also showed variance on the dependent construct, with response efficacy showing 10 percent explained by threat susceptibility and threat severity perception. In contrast, the independent constructs showed variance on the dependent construct, with self-efficacy showing only 8 percent explained by threat susceptibility and perception of threat severity. Computer security usage showed 67 percent explained by protection motivation (see Figure 2; Appendix H).

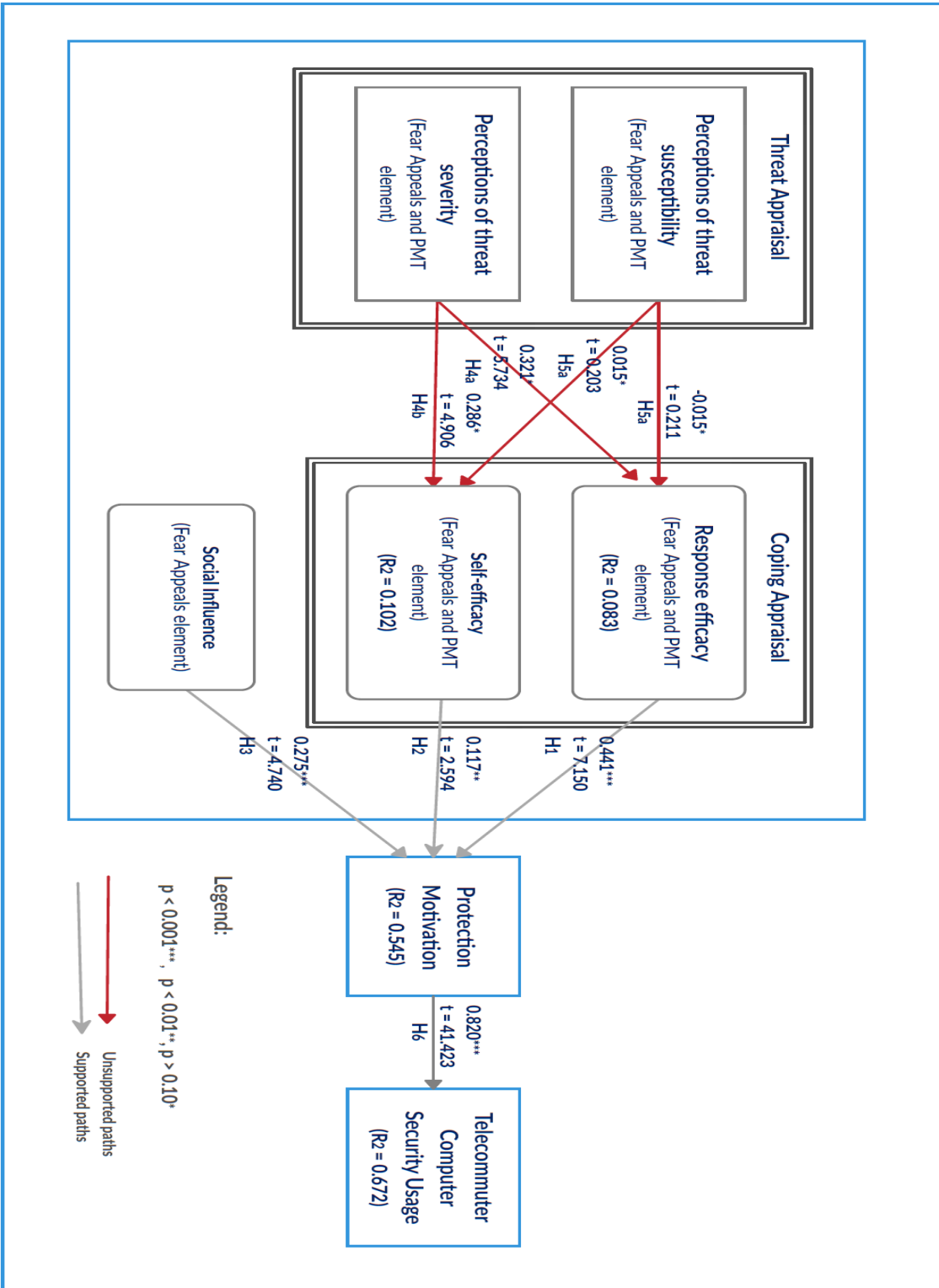


Figure 2. PLS Analysis Result for Computer Security Usage

Based on Mertler and Reinhart (2017), the recognized benchmark for outliers is a value for Mahalanobis distance that is much further away from $p < .001$, determined by evaluating the calculated Mahalanobis distance to the chi-square critical value. Response efficacy ($\beta=0.441$, $p<0.001$) showed a significant and direct positive effect on protection motivation, in support of **H₁**, and self-efficacy ($\beta=0.117$, $p<0.05$) showed a positive effect on protection motivation **H₂**, though not as strong as a response efficacy on protection motivation. Thus, **H₁** and **H₂** of the hypotheses were supported. Also, the **H₃** on social influence ($\beta=0.275$, $p<0.001$) did show a significant effect on protection motivation. The two perceived threat severity constructs in this study had significant and positive effects on **H_{4a}** response efficacy ($\beta=0.321$, $p<0.001$) and **H_{4b}** self-efficacy ($\beta=0.286$, $p<0.001$), instead of negative effects as proposed. Thus, **H_{4a}** and **H_{4b}** were not supported. The two perceived threat susceptibility constructs had no effects on **H_{5a}** response efficacy ($\beta=-0.015$, $p>0.100$) and **H_{5b}** self-efficacy ($\beta=0.015$, $p>0.100$). Hence, **H_{5a}** and **H_{5b}** were not supported, while **H₆** protection motivation ($\beta=0.821$, $p<0.001$) had a substantial and direct positive effect on computer security usage. Thus, **H₆** of the hypotheses was significantly supported (see Table 6).

Table 6

Summary of Hypotheses Tests

Hypothesis (with Direction)	Path Coefficient (β)	<i>t</i> Value	<i>p</i> Value	Support
H₁ : Response Efficacy -> Protection motivation	0.441	7.150	0.000	Yes
H₂ : Self-Efficacy -> Protection motivation	0.117	2.594	0.010	Yes
H₃ : Social Influence -> Protection motivation	0.275	4.740	0.000	Yes
H_{4a} : Perceived Threat Severity -> Response Efficacy	0.321	5.734	0.000	No - significant effect in opposite direction
H_{4b} : Perceived Threat Severity -> Self-Efficacy	0.286	4.906	0.000	No - significant effect in opposite direction
H_{5a} : Perceived Threat Susceptibility -> Response Efficacy	-0.015	0.211	0.833	No

H5b: Perceived Threat Susceptibility -> Self-Efficacy	0.015	0.203	0.839	No
H6: Protection motivation -> Computer Security Usage	0.820	41.423	0.000	Yes

Summary of Hypotheses Results

H1: Response efficacy had a significant positive effect on a telecommuter's computer security protection motivation.

H2: Self-efficacy positively affected a telecommuter's computer security protection motivation.

H3: Social influence had a significant positive effect on a telecommuter's computer security protection motivation.

H4a: Perceptions of threat severity did not have a negative impact on response efficacy but had a significant positive influence on the perceptions of response efficacy.

H4b: Perceptions of threat severity did not have a negative impact on self-efficacy and instead had a significant positive influence on the perception of self-efficacy.

H5a: Perceptions of threat susceptibility did not influence perceptions of response efficacy.

H5b: Perceptions of threat susceptibility did not influence perceptions of self-efficacy.

H6: An increase in protection motivation significantly improves the computer security behaviors of telecommuters working with sensitive data.

Chapter 5

Conclusions

From the outcomes of the survey data evaluated as portrayed in Chapter 4 (Figure 2), perceptions of threat severity did not have a negative effect on response efficacy and self-efficacy as anticipated. It can be deduced from these findings that confidence in the effectiveness of computer users of the available response efficacy and their self-efficacy to protect their computers helps them diminish or reject the severity of perceived threats. The response efficacy of the computer users is an essential aspect that guides them to take security actions to protect their computers from viruses and prevent data breaches when working at home with confidential data. Also, Posey et al. (2015) deemed threat susceptibility to be a critical factor in the threat appraisal process and the general formation of insiders' protection motivation. Herath and Rao (2009) observed that a person's protection motivation is centered on the perceived vulnerability to the threat. According to Workman et al. (2008), the assessment of being susceptible to threats precedes an evaluation of coping appraisals that motivate users to protect themselves.

Additionally, computer users considered the response efficacy of the security actions presented to mitigate viruses and data breach threats from the outcomes. The findings of the study are not contrary to the literature. Posey et al. (2015) stressed that response efficacy was more significant than the threat appraisal constructs showed a more considerable role in establishing protection motivation. Johnston and Warkentin (2010) likewise noted that moderate to high response efficacy levels are related to positive tendencies of threat mitigation in which a recommended response is sanctioned. Also, prior literature substantiated the outcome. Davis et al. (1989) suggested that an important predictor of protection motivation is response efficacy. In agreement with earlier results of studies, the outcomes of the study showed that security

measures of social influence affect protection motivation of computer users to secure their computers.

The relationship shown by social influence in the study can be credited to the significant impact of response efficacy, and self-efficacy have on protection motivation. Per Boss et al. (2015) and Posey et al. (2015), in the coping appraisal process of PMT, response efficacy and self-efficacy must be greater than social influence for a person to employ protection motivation. From the study's findings, it was evident that response efficacy and self-efficacy of computer users did not outweigh their social influence to engage in protective behavior. Hence, it can be deduced that computer users are very confident in their response efficacy and self-efficacy against security threats, with their social influence significantly influencing their protective security behavior. The telecommuters accessing sensitive data were confident in their response efficacy and self-efficacy. As portrayed by the outcomes, the self-efficacy considerably influenced users motivation to protect their computers from malware and viruses as they work at home with access to confidential information. The result conformed to the literature. Posey et al. (2015) postulated that self-efficacy is a more considerable predictor of protection motivation in various circumstances, while Keith et al. (2015) noted that adopting the self-efficacy construct presents a more thorough method to comprehend the protection behavior of computer users. Self-efficacy has a significant positive impact on behavior of users to protect themselves (Johnston & Warkentin, 2010).

Individuals' computer security usage is considerably spurred by their motivation to protect their computers from spyware, viruses, and data breaches. The current literature completely confirms this finding. Posey et al. (2015) suggested that the impact of protection motivation on behavior is significant and positive. Johnston and Warkentin (2010) stressed that

when threat appraisals and coping appraisals are at moderate-to-high levels, an individual's protection motivation is likewise increased, thereby significantly influencing actual behavior. The stronger the determination to comply with security measures, the greater the actual compliance prospect (Pahnila et al., 2007). Rogers (1983) theorized that protection motivation is the variable that propels amendment in behavior.

Discussion

The study addressed whether persuasive communication via the FAM might alter security behavior of telecommuters working with confidential data. To what extent did self-efficacy, response efficacy, threat severity, perceived threat severity, perceived threat susceptibility, and social influence impact security behavior of users when working from home? When the entire study question was examined, the findings revealed that individuals' security behavior influenced response efficacy, self-efficacy, and social influence.

Surprisingly, the two hypotheses **H_{4a}** and **H_{4b}** were not supported, involving threat severity but significantly influenced response efficacy and self-efficacy positively instead of negatively. The perceived threat severity believes that a person involved with Fear Appeals harbored the threat's significance (Rogers 1975; Witte, 1992). PMT defines threat severity assessments as controlling the intensity of response. The assessment is done by clearly controlling perceptions of both response efficacy and self-efficacy. When the telecommuter working with confidential data was considered, this population may have been inundated with security situations. The prior exposure to security measures due to the nature of their jobs may not have changed their perception of the secured users in the home office environment.

The hypothesis **H_{5a}** and **H_{5b}** for threat susceptibility did not impact response efficacy and self-efficacy. On the contrary, Johnston and Warkentin (2010) found that perceived threat severity negatively impacted response efficacy and self-efficacy. This study's results corresponded with that of Johnston et al. (2015) in their use of Fear Appeals. They contended that the rationale for these non-conforming outcomes was from the orthodox Fear Appeals linguistic framework and the wrong depiction of FAM in the information security literature. Academics have always neglected the core postulation that the adopted threats should have individual significance for the Fear Appeal crowd. The standard Fear Appeal language did not describe the discrepancy between threats to an individual and threats to that individual's data. The **H_{5a}** and **H_{5b}** for threat susceptibility did not influence telecommuters because this group of the population was not susceptible to threats and had taken some drastic measures to safeguard the confidential data as they work with from home.

While some telecommuters could be further motivated by protection and others may be inspired more by the need to avert individual pain via unofficial measures, the aggregate impact of mixing both elements would be encouraging (Johnston et al., 2015). The insignificant influence of threat susceptibility could be due to the notion that the telecommuters working with confidential data did not feel vulnerable since they may have taken most of all the necessary steps to secure their computers. This situation could be characterized as threat susceptibility fatigue. The user working at home with sensitive information may already have anti-virus or antispyware installed on their computers.

Computer response efficacy showed a significant positive relationship with protection motivation at a value of $t = 7.150$. For the first sub-question, it was found that there was a statistically significant R^2 change of .102 between response efficacy and protection motivation.

Therefore, one can state that there was a significant relationship between response efficacy and security behavior. The telecommuters indicated they could efficiently respond to information about security threats.

Computer self-efficacy particularly showed a strong relationship with protection motivation at a value of $t = 2.594$. This implies that the level of motivation for computer users to undertake positive protective measures that will fortify their computers is profoundly driven by their assessment of the probability of being vulnerable to these threats, the level of confidence in the mitigating controls, and in their own abilities to use the mitigating controls adequately.

Computer social influence indicated a strong relationship with protection motivation at a value of $t = 4.613$. Therefore, one can determine a significant relationship between social influence and security behavior. The responsibility of social groups or anticipation can modify a person's response to behave as anticipated by individuals or groups that favor secure computer protective action of a telecommuter. This indicates that a home computer user's security awareness for their computers relies on the situation and social influences, impacting their decisions (Herath & Rao, 2009).

Computer security usage is explained by protection motivation at 67 percent. Protection motivation had a large t -value of 41.423, which is well above the acceptable value of 1.96 suggested by Hair et al. (1995). This implies that computer security usage is based on the motivation of users to protect their computers from malware security threats. This study presented theoretical implications and contributes to the IS security domain literature, primarily filling the existing gap by explicitly changing the work environment, confidential data, and associated security threats.

Johnston and Warkentin (2010) asserted that the purpose of their study was to investigate the influence of Fear Appeals on the conformity of computer users with suggestions to enact specific individual computer security actions toward the mitigation of threats. Their study's outcomes showed that Fear Appeals did influence the user's security behavioral intentions. It was also realized that the effect was not the same among all computer users, mainly since it depended on the interpretation of fear arguments. Some individuals found the warning messages to be motivating, and they were encouraged to avert that consequence, while some were not receptive to this form of communication (Johnston & Warkentin, 2010).

The purpose of the study was to identify if the FAM's use would be an effective form of persuasive communication and whether that could change the security behavior of telecommuters working with sensitive data. The FAM has several variables that make it unique. The inclusion of response efficacy (the notion that taking a particular course of action will have an impact), self-efficacy (the notion that the user can make a difference by following the suggested course of actions), and social influence (altering behavior centered on what others might think of you) make the fear appeals model potential and robust way for management to communicate with their staff. The Fear Appeals communication should not only be used to train employess but to possibly put a set of consequences in place if the policies were not followed.

Some studies investigated the usage of computers in unusual ways in areas such as education (Martin & Ertzberger, 2013), finance (Fenu & Pau, 2015), and healthcare (Boruff, & Storie, 2014). The results contribute to the current literature by demonstrating the effects of perceived threat severity, perceived threat susceptibility, social influence, response efficacy, self-efficacy, and protection motivation on the actual information security usage behavior of

computer users at home working with confidential data in the context of malware and data breach, an uncharted research area.

Furthermore, the emphasis on actual security usage behavior adds to the existing literature by demonstrating that telecommuter's computer protection from malware and data breach transcends the intention of the users to actual behavior. Intention serves as a precursor of behavior, and there is an anticipation that users fulfill their intentions (Ajzen, 1985). Several past studies in the IS security domain relied on behavioral intention as the dependent variable (Johnston & Warkentin, 2010; Yoon & Kim, 2013). The research contributes to those earlier results and the existing literature via the insertion of computer security usage as a dependent construct that centers on actual security behavior.

The reliance on intentions in prior information security studies, instead of actual behavior, hindered theory advancement and validation (Crossler et al., 2013). Boss et al. (2015) also indicated that actual behaviors are vital in information security research since the aim is to alter security behaviors, not only security intentions. An additional theoretical consequence of these findings is that it strengthens the capability of FAM to forecast the behavior of users founded on threat and coping appraisals. Boss et al. (2015) and Posey et al. (2015) suggested that the FAM is centered on both threat and coping appraisals and how these factors affect protection motivation. As presented in Figure 1, the extended FAM recommended that users take suggested responses to threats, particularly in computer security usage concerning malware viruses and data breach. The utilization of the computer security usage construct and the study's ensuing findings adds to the literature by accentuating how actual security behavior of users applying computer security features to enhance protection against malware, virus, and data breach. This

finding re-emphasizes the importance of actual behavior in the IS security literature and research (Boss et al., 2015; Crossler et al., 2013).

Further theoretical consequence of this study is that it extends the use of FAM to a comparatively unfamiliar but relevant area in the IS security realm. Hence, a realistic evaluation of the information security behavior of telecommuters in the context of malware and data breach when they work with confidential information was assessed with FAM and PMT. The widespread susceptibilities of computers to a virus and other malware contrasted with typical systems (Li & Clark, 2013; Tu & Yuan, 2012) and the demand for users to follow extraordinary procedures to lessen or avert them (Tu and Yuan, 2012; Tu et al., 2015). The FAM's use reinforces its capacity to be engaged in various user information security behavior settings. Herath and Rao (2009) remarked that PMT could be studied and employed in various information security situations.

There are pragmatic outcomes of the study; a realization that protection motivation significantly impacted computer security behavior for the home office user working with sensitive data. There is an indication of the influence of self-efficacy on protection motivation. The inference is that experts should devise information security training programs to focus on computer self-efficacy of telecommuters with access to confidential information. Hence, an ongoing enhancement of information security skills of users to keep abreast with computer technology and improves their skills to leverage it continuously. There should be more regular computer training as computer technology is always changing (Harris et al., 2014). The security training of computer users should include awareness of the vulnerability of computers to the threats of a virus, malware, phishing, malicious website sites, and some applications (Edwards, 2015). The additional practical inference of the study is that experts should model computer

management systems with procedures and techniques that empower users to take realistic steps to protect their devices.

The study was conducted with telecommuters; the results can be a wide-ranging concept that might apply to all home computer users in the United States. The individuals involved in the study who met the inclusion criteria indicated their activities from a telecommuter's viewpoint working with confidential data. Previous studies have indicated that home behavior is ubiquitous work behavior, and consequently, a link can be drawn between the two. The sample exemplifies the overall United States population who utilize a home computer and work with sensitive data. Since no industries were differentiated, these results are applicable, in general, to all businesses where one can work from home with access to confidential data. It is also remarkable that spyware and anti-spyware were treated as a substitute for malware and countermeasures against malware, a considerable concern in securing company network if one assumes that home computer users may be telecommuting.

These results corroborate the firm notion that the FAM can be a useful form of persuasive communication for management when working with their employees. The study was based precisely on telecommuters, but human behavior is frequently pervasive if one is working on their personal computer at home or with work behavior, and the findings extend in terms of computer security. Reeducating the workforce centered on a violation, applying a set of penalties, or having some degree of responsibility for actions, means that the FAM's utilization can alter behavior of telecommuters when it concerns security issues. When concentrating mainly on threat severity, the evidence on fear appeals is not transformed into the design of computer information security messages. Existing data shows that information about the severity of potential negative effects from threat behavior might trigger protective responses. These

counterproductive responses might be averted by instructing how to effectively implement the suggested measures and persuade individuals to be vulnerable to the threat.

While productivity-based software tools such as worksheets and word processors can improve job performance, many security technologies impede performance (Warkentin et al. 2004; Warkentin et al. 2007) to secure the working environment. The basis for threatening actions, such as viral attacks and spyware plagues, is more unyielding or plausible. Computer users may begin to question their competence to function sufficiently in the intensified threat circumstances, devoid of a data breach or computing setting. More et al. (1990) contended that high degrees of emotional awakening is related to reduced computer user performance. To underscore the severity of spyware, assertions that explain its potential to expose sensitive information or hamstring the computer's performance were incorporated into the Fear Appeal treatment. Furthermore, individual outcomes, such as computer virus infections, were conveyed in the message by portraying the potential for identity theft or fraud (Johnston & Warkentin, 2010).

Also involved in this evaluation for semblance are the formative variables performance expectancy and attitude on antispayware usage (Shaw & Wright, 1967). A person's protection motivation would likewise be at a moderate-to-high level, thus boosting the likelihood of a shift in attitude and behavior (Johnston & Warkentin, 2010). These kinds of fear-stimulating persuasive messages have been demonstrated to motivate alterations in attitude, behavioral intent, and behavior (Schneider et al. 2001; Sherer & Rogers, 1984). The study followed this method and did not incorporate attitude into the theoretical model. Attitude and performance had little impact on behavior, as indicated in the outcomes (see Appendix I).

Limitations and Future Studies

The research was limited to information security behavior of computer users, and within the aspect of computer security, the study extended the restricted constructs that represents the FAM core nomology. The study results unpredictably showed that social influence of security actions was inspired by the level of motivation to protect computers from data breaches and malware. Therefore, it is recommended that future studies in computer security pay particular attention to social influence and study this construct further.

The data gathered for this study were limited to telecommuters in the United States of America. It is suggested that future studies should widen and diversify the populations from which data gathered will consist of other geographic regions and the United States of America. Furthermore, future studies must reflect data gathering from populations sampled on the use of culture, as a study invoking such data conditions in this area of user information security behavior might expose some remarkable outcomes. Also, online surveys have the limitation of self-selection bias when potential respondents decide whether to participate in the survey, and the group that chooses to participate is not equivalent to the group that opted out. This drawback impacts the extension of the outcome to the general population examined.

Summary

The study's premise was to identify and define an existing information system problem. Hence, an empirical assessment of information security usage behavior of computer users in the context of a data breach was examined. The background of the study was introduced at the beginning of the research. After a review of the literature, the study pursued to evaluate the impact of that perceived threat severity, perceived threat susceptibility, perceived social influence, response efficacy, and computer self-efficacy have on influencing the protection

motivation of telecommuters working with confidential data and determined how that guides their usage of computer security. The research question was proposed and established to advance hypotheses and an intended research model.

The impediments and concerns encountered in the effort to recommend an answer to the question were introduced. The review of literature underscored and integrated literature from earlier studies and sources that assessed user information security behavior. The theoretical foundation was based Fear Appeals Model (FAM) and Protection Motivation Theory (PMT). The PMT establishes the foundation of the theoretical model (FAM) examined in the study, but since the proposed solution to a security threat is frequently technology-focused, the social influence and computer security usage were added (Johnston & Warkentin, 2010). The study noted that PMT showed protection motivation of individuals was grounded on perceived threats and their situations, how the persons coped with the threats based on two activities: threat appraisal and a coping appraisal in which the decisions to diminish or alleviate the threats were evaluated.

Generally, the literature review presented the constructs, results, and contributions from prior literature, including existing gaps that necessitated further study. The design used was depicted in the Research Method chapter. The quantitative survey method approach was deemed appropriate and used. The survey instrument's reliability and validity, sample data, and data collection methods were discussed. The nonprobability sampling design was utilized since data were gathered from a particular group, particularly telecommuters working with sensitive data.

Data analysis was accomplished using SPSS and Smart PLS 3.0. The statistical tests performed involved Mahalanobis distance, normality, factor analysis, construct reliability and validity, PLS algorithm, and bootstrapping. The interpretation of the numerous outcomes from

the statistical tests is depicted in chapter 4 and the appendices. The acceptance or rejection of the hypotheses was centered on assessing the statistical findings. The final chapter stated the implications of the results, recommendations, limitations, and future study suggestions. The emphasis and outcomes are considered to have shed more light on information security behavior of computer users in general and telecommuters working with confidential information in the context of malware, virus, and data breach.

The study has strengthened the awareness of elements that motivates computer users to protect their computers. Hence, it underscored the cognitive process that precedes computer security's actual usage by telecommuters. Moreover, extended FAM with computer security to develop a research paradigm provides more awareness of the current literature. The findings shed light on this continuing debate as it emphasizes how computer users, who exert independence in their security decision, make and act to secure their computers from threats.

It is suggested that organizations, specifically those that use computers, understand how employees handle security threats and their computer security usage. Since the outcomes of this study show that computer security usage is based on personal behavior, it is also suggested that establishments emphasize the cognitive aspects of users more via information security awareness programs, instead of exclusively trusting the conventional compliance approach, which is based only on organizational security policies. Ultimately, the research construct advanced will provide a vivid foundation for potential studies seeking to extend the FAM constructs in other domains of study in computer security.

Appendices

Appendix A:

IRB Approval



MEMORANDUM

To: Titus Fofung
College of Engineering and Computing

From: Cristina Garcia-Godoy, D.D.S., M.P.H., C.C.R.P.
Chair, Institutional Review Board

Date: October 22, 2020

Subject: IRB Exempt Initial Approval Memo

TITLE: Examination of the Computer Security Behaviors of Telecommuters Working with Confidential Data through Leveraging the Factors from Fear Appeals Model (FAM)–NSU IRB Protocol Number 2020-501

Dear Principal Investigator,

Your submission has been reviewed and approved by the Institutional Review Board on **October 20, 2020**. You may proceed with your study.

Please Note: If you receive stamped copies of consent, assent, and recruiting materials indicating approval date, these documents must be used when recruiting and consenting or assenting participants.

Level of Review: Exempt

Type of Approval: Initial Approval

Exempt Review Category: Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

Post-Approval Monitoring: The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

Page 1 of 2

Final Report: You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the IRB Closing Report Form.

Translated Documents: No

Please retain this document in your IRB correspondence file.

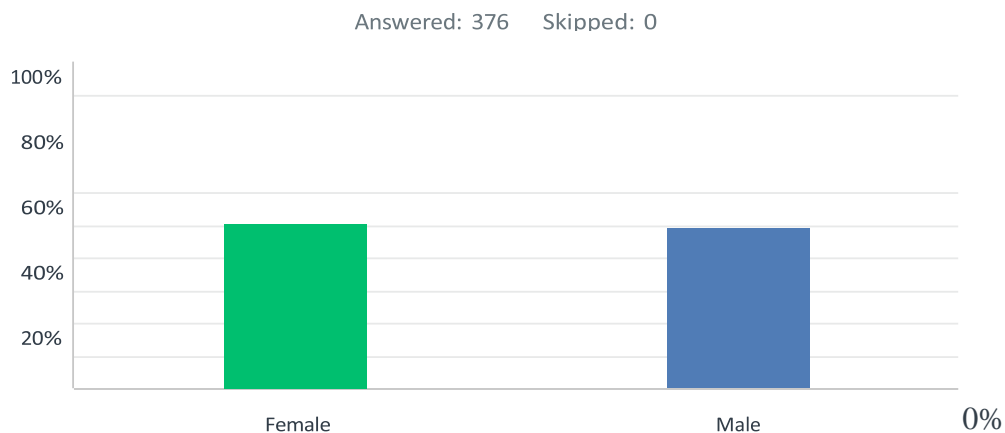
CC: Ling Wang, Ph.D.

Ling Wang, Ph.D.

Appendix B:

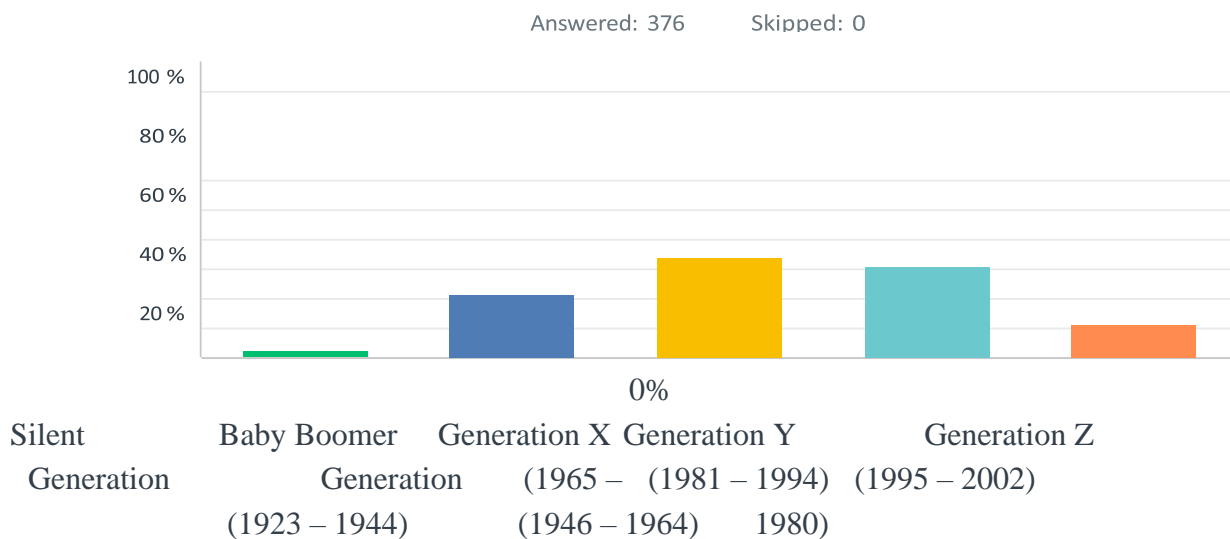
All data descriptive

Q1 What is your gender?



ANSWER CHOICES	RESPONSES	
Female	50.80%	191
Male	49.20%	185
TOTAL		376

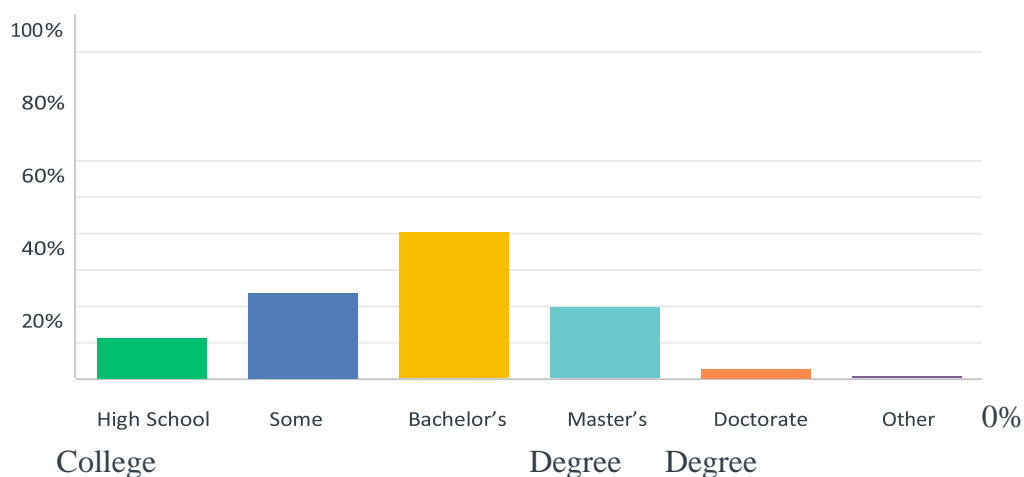
Q2 Select the interval that represents your year of birth.



ANSWER CHOICES	RESPONSES	
Silent Generation (1923 – 1944)	2.39%	9
Baby Boomer Generation (1946 – 1964)	21.54%	81
Generation X (1965 – 1980)	33.78%	127
Generation Y (1981 – 1994)	30.85%	116
Generation Z (1995 – 2002)	11.44%	43
TOTAL		376

Q3 What is the highest level of education you have completed?

Answered: 376 Skipped: 0

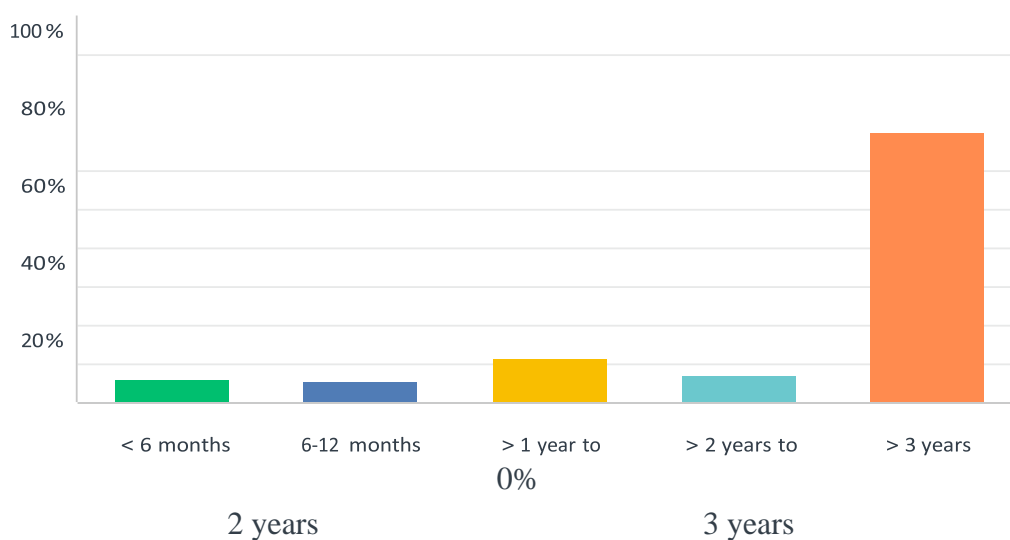


ANSWER CHOICES	RESPONSES	
High School	11.44%	43
Some College	23.94%	90
Bachelor's Degree	40.43%	152
Master's Degree	20.21%	76

Doctorate	3.19%	12
Other	0.80%	3
TOTAL		376

Q4 How long have you been using a computer for work?

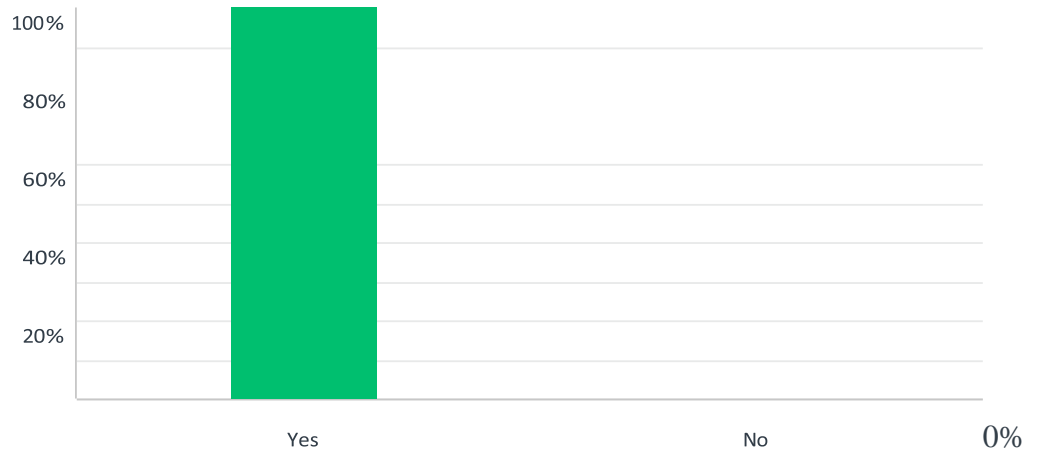
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES
< 6 months	6.12% 23
6-12 months	5.32% 20
> 1 year to 2 years	11.70% 44
> 2 years to 3 years	6.91% 26
> 3 years	69.95% 263
TOTAL	376

Q 5 Do you work from home?

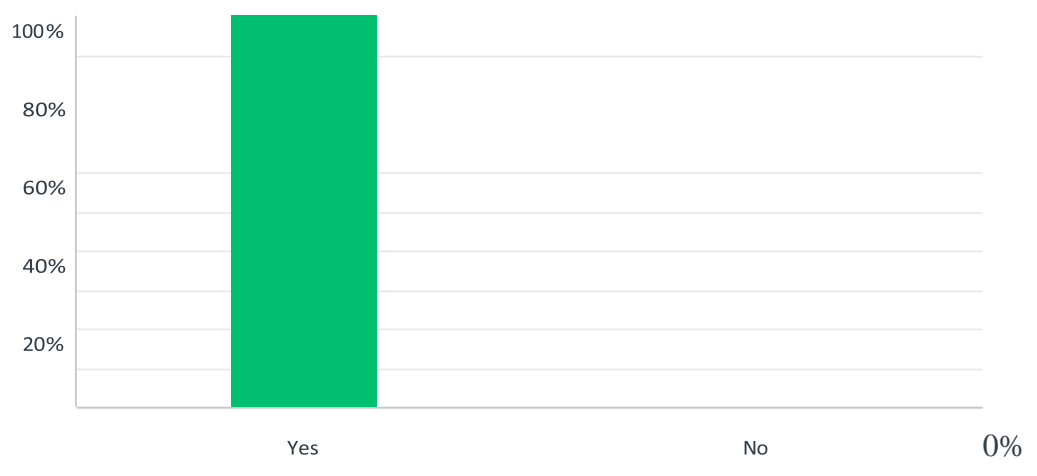
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Yes	100.00%	376
No	0.00%	0
TOTAL		376

Q 6 Do you work with sensitive, private or confidential data?

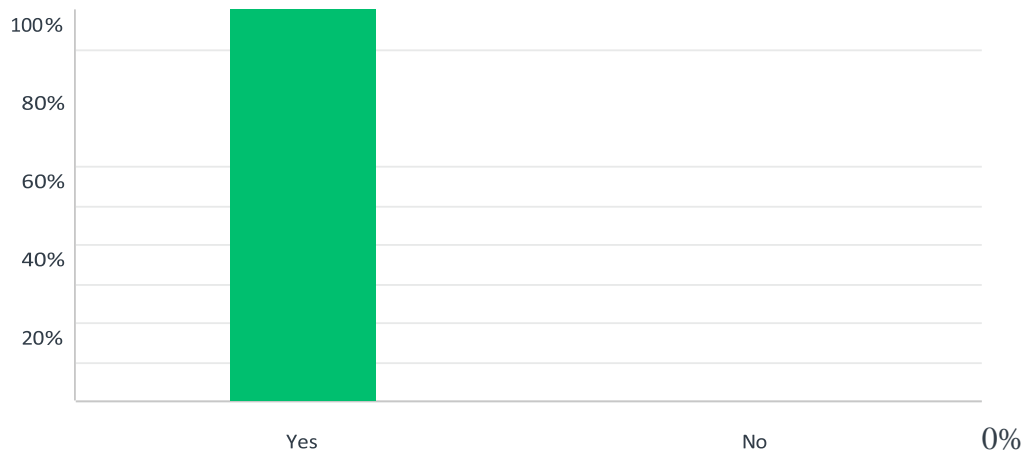
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES
Yes	100.00% 376
No	0.00% 0
TOTAL	376

Q 7 Do you have anti-virus installed on your computer?

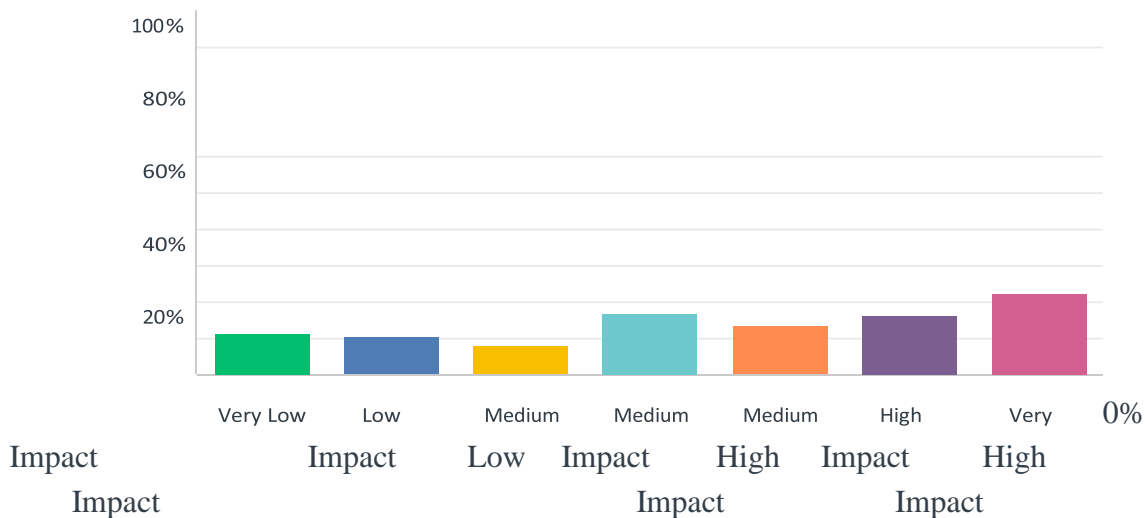
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES
Yes	100.00% 376
No	0.00% 0
TOTAL	376

Q8 My computer was infected by spyware.

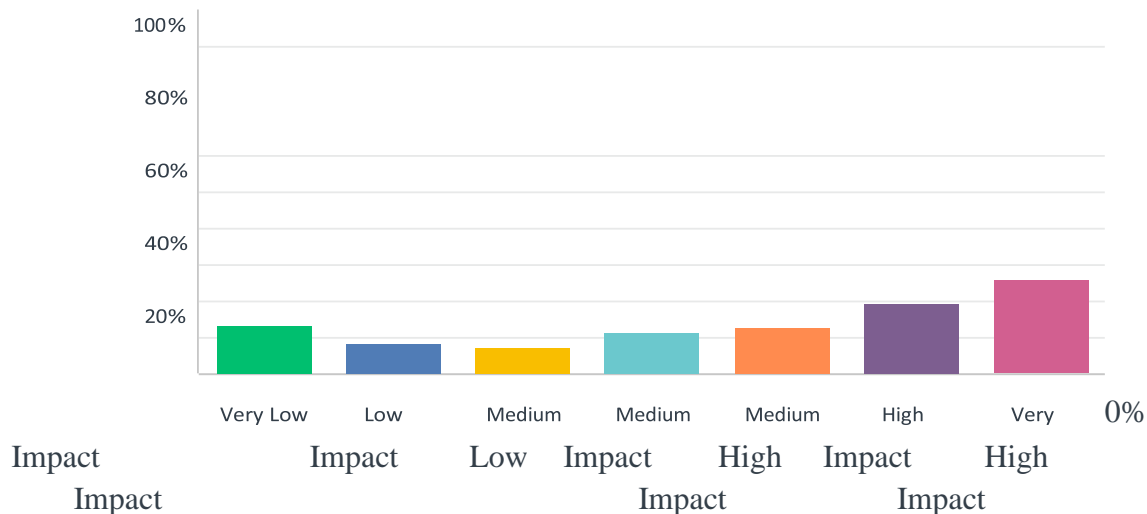
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Very Low Impact	11.70%	44
Low Impact	10.64%	40
Medium Low Impact	8.24%	31
Medium Impact	17.02%	64
Medium High Impact	13.30%	50
High Impact	16.49%	62
Very High Impact	22.61%	85
TOTAL		376

Q9 My computer is becoming corrupted by a virus.

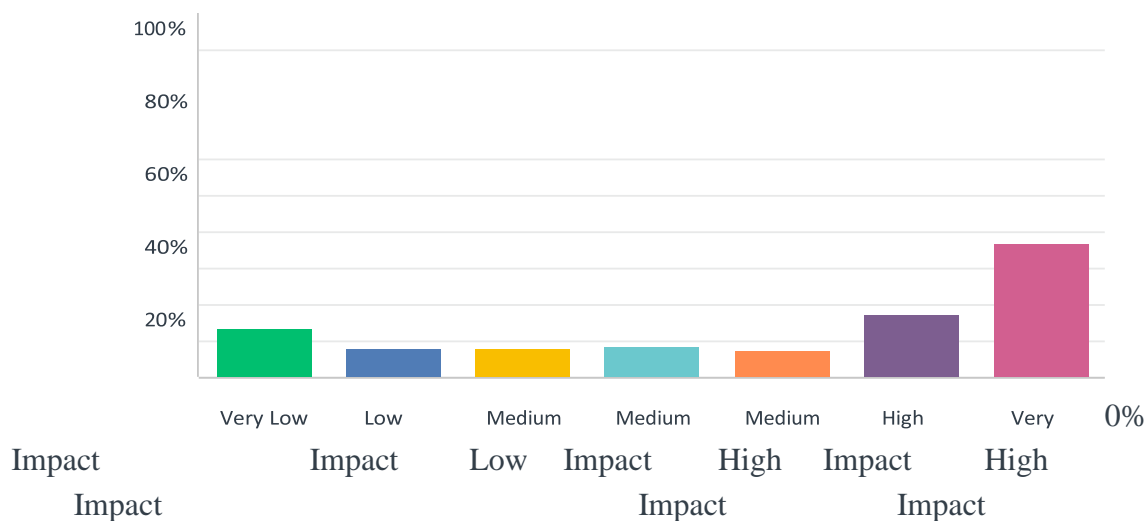
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Very Low Impact	13.56%	51
Low Impact	8.51%	32
Medium Low Impact	7.71%	29
Medium Impact	11.70%	44
Medium High Impact	12.77%	48
High Impact	19.68%	74
Very High Impact	26.06%	98
TOTAL		376

Q10 My computer being taken over by a hacker.

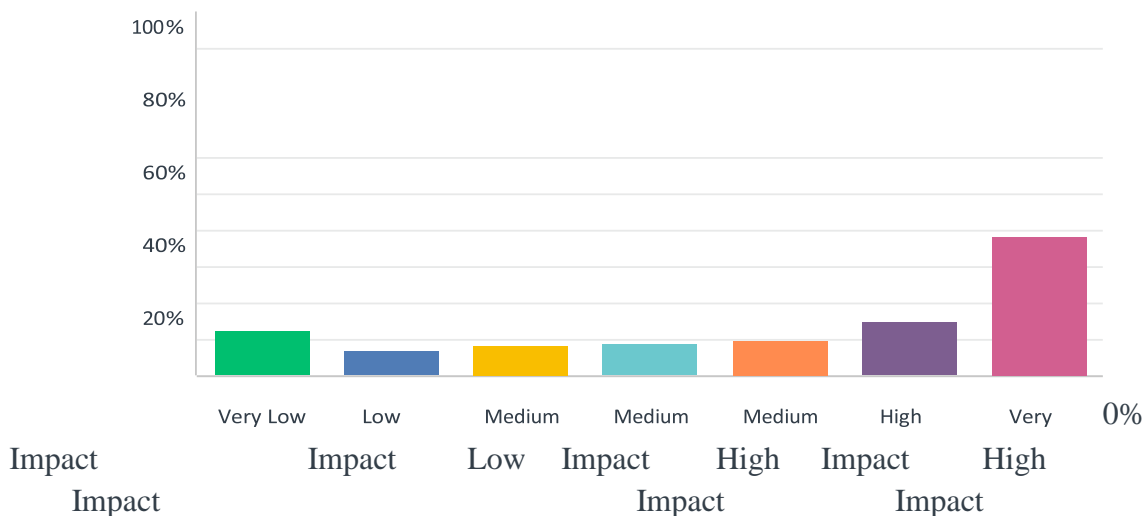
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Very Low Impact	13.30%	50
Low Impact	8.24%	31
Medium Low Impact	7.98%	30
Medium Impact	8.51%	32
Medium High Impact	7.71%	29
High Impact	17.29%	65
Very High Impact	36.97%	139
TOTAL		376

Q11 Sensitive data being stolen from my computer.

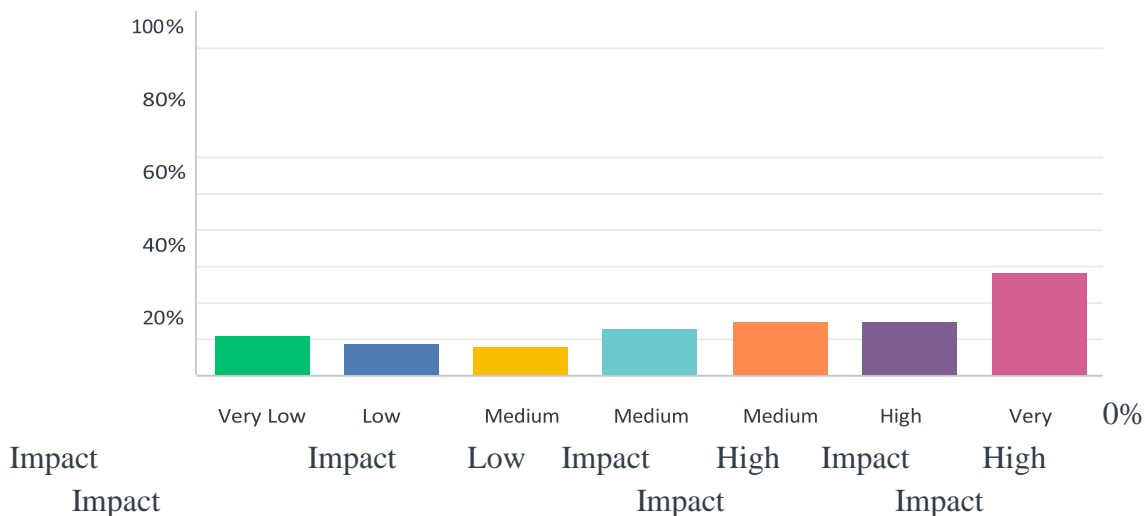
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Very Low Impact	12.50%	47
Low Impact	6.91%	26
Medium Low Impact	8.51%	32
Medium Impact	8.78%	33
Medium High Impact	9.84%	37
High Impact	14.89%	56
Very High Impact	38.56%	145
TOTAL		376

Q12 Sensitive data being lost due to a virus on my computer.

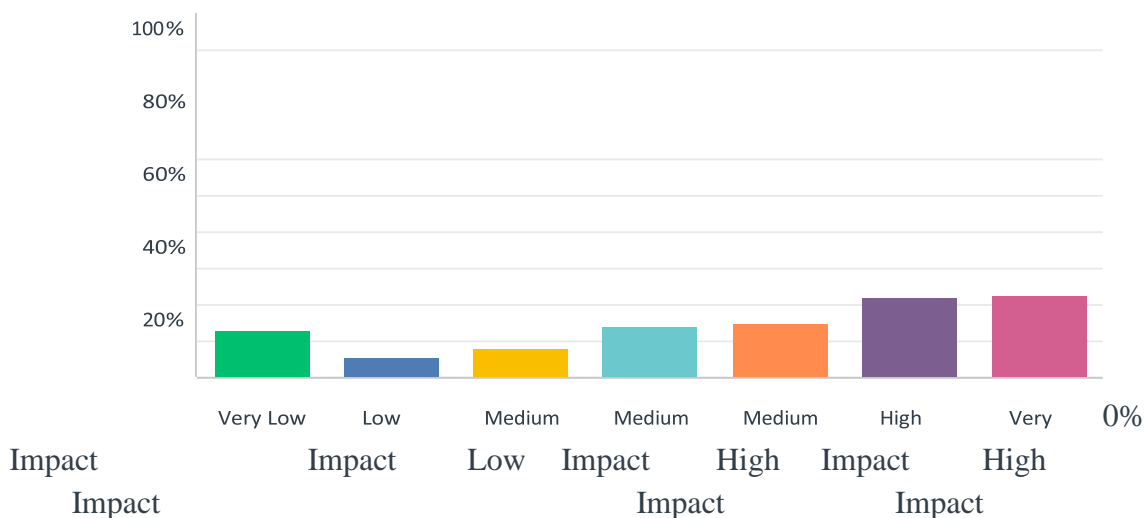
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Very Low Impact	11.17%	42
Low Impact	9.04%	34
Medium Low Impact	7.98%	30
Medium Impact	13.03%	49
Medium High Impact	14.89%	56
High Impact	15.16%	57
Very High Impact	28.72%	108
TOTAL		376

Q13 My computer is downloading a virus or an application with many bugs.

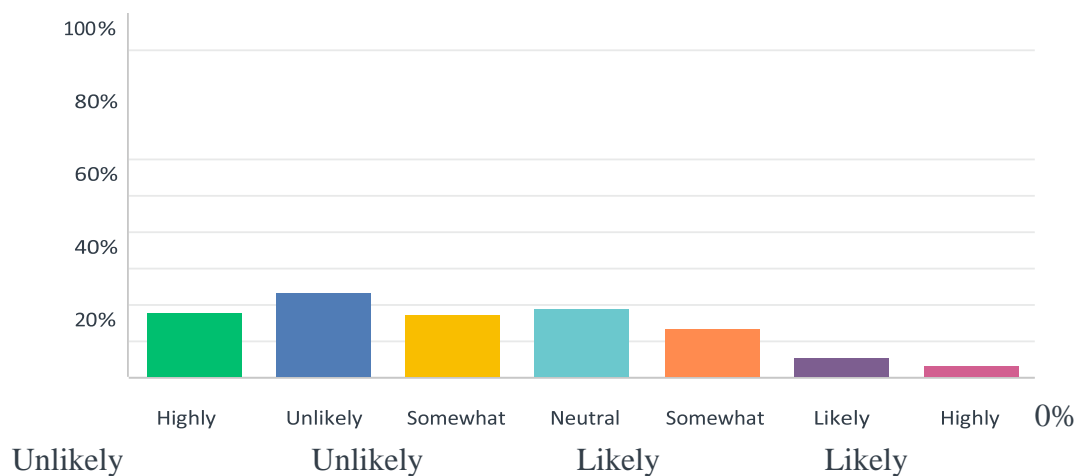
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Very Low Impact	13.03%	49
Low Impact	5.59%	21
Medium Low Impact	7.98%	30
Medium Impact	14.10%	53
Medium High Impact	14.89%	56
High Impact	21.81%	82
Very High Impact	22.61%	85
TOTAL		376

Q14 My computer is at risk of becoming infected with spyware.

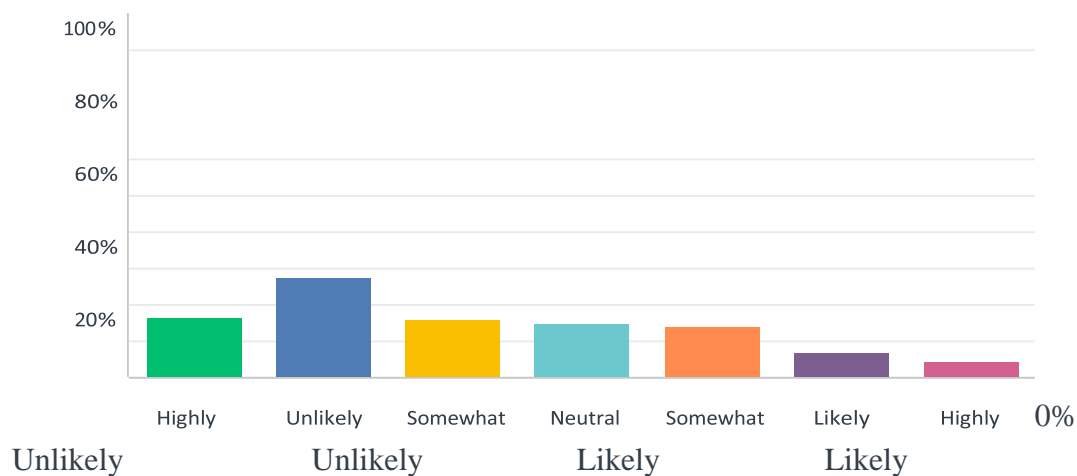
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES
Highly Unlikely	18.09% 68
Unlikely	23.40% 88
Somewhat Unlikely	17.29% 65
Neutral	18.88% 71
Somewhat Likely	13.30% 50
Likely	5.32% 20
Highly Likely	3.72% 14
TOTAL	376

Q15 My computer will likely become infected with spyware.

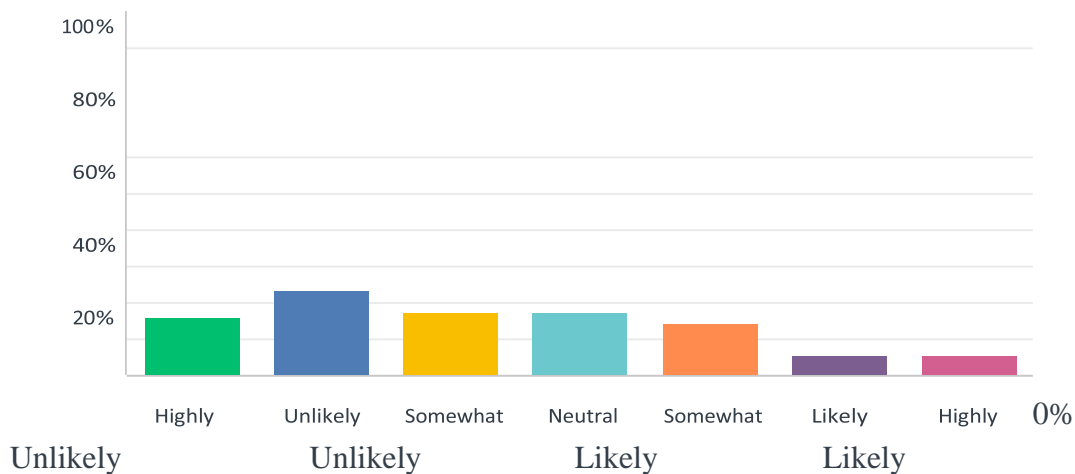
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Highly Unlikely	16.49%	62
Unlikely	27.66%	104
Somewhat Unlikely	15.96%	60
Neutral	14.89%	56
Somewhat Likely	13.83%	52
Likely	6.91%	26
Highly Likely	4.26%	16
TOTAL		376

Q16 My computer may become infected with spyware.

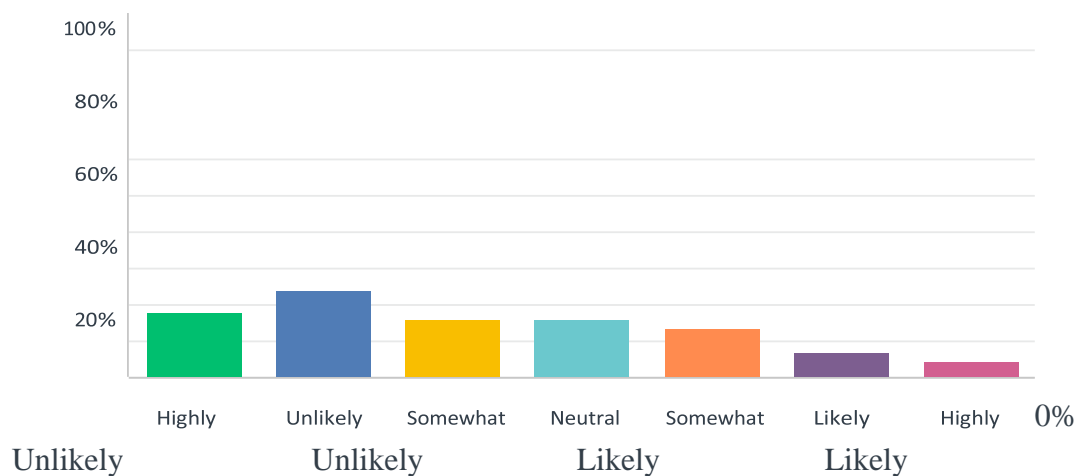
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Highly Unlikely	16.22%	61
Unlikely	23.67%	89
Somewhat Unlikely	17.29%	65
Neutral	17.55%	66
Somewhat Likely	14.36%	54
Likely	5.59%	21
Highly Likely	5.32%	20
TOTAL		376

Q17 My computer becoming corrupted by a virus.

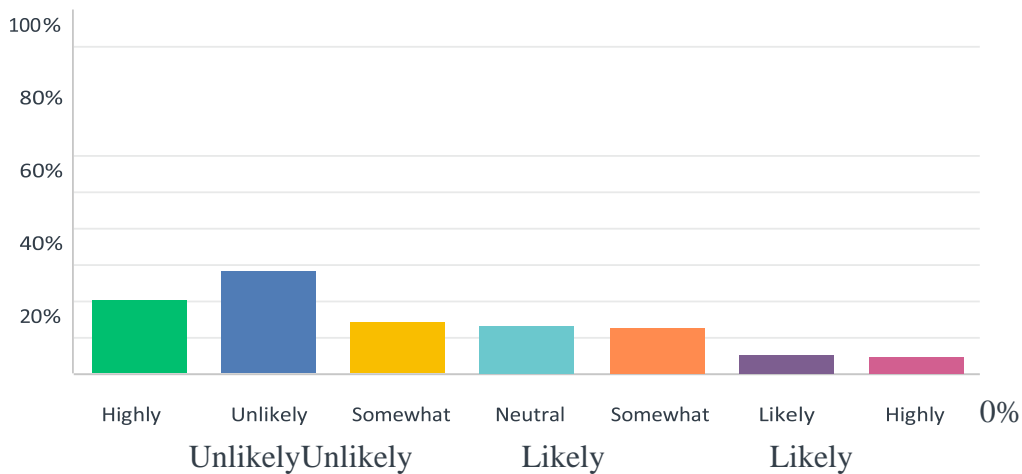
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES
Highly Unlikely	18.09% 68
Unlikely	24.20% 91
Somewhat Unlikely	16.22% 61
Neutral	16.22% 61
Somewhat Likely	13.56% 51
Likely	7.18% 27
Highly Likely	4.52% 17
TOTAL	376

Q18 My computer being taken over by a hacker.

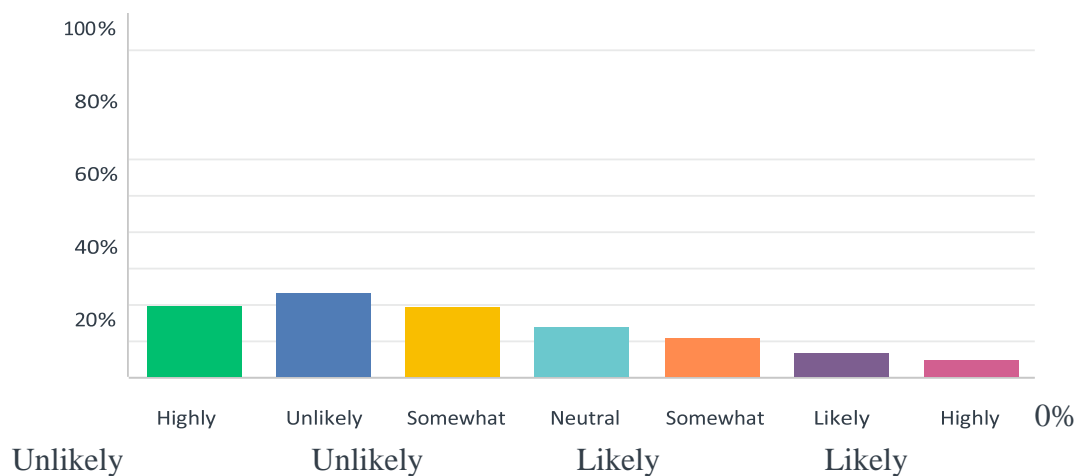
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES
Highly Unlikely	20.74% 78
Unlikely	28.46% 107
Somewhat Unlikely	14.36% 54
Neutral	13.30% 50
Somewhat Likely	12.77% 48
Likely	5.59% 21
Highly Likely	4.79% 18
TOTAL	376

Q19 Sensitive or confidential data being stolen from my computer.

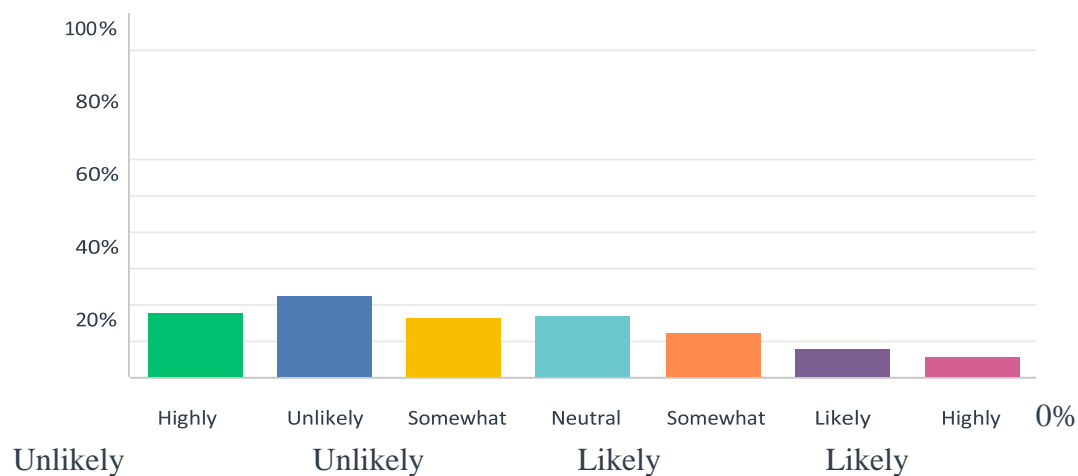
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Highly Unlikely	19.95%	75
Unlikely	23.40%	88
Somewhat Unlikely	19.41%	73
Neutral	14.10%	53
Somewhat Likely	11.17%	42
Likely	6.91%	26
Highly Likely	5.05%	19
TOTAL		376

Q20 Sensitive or confidential data is lost due to a virus on my computer.

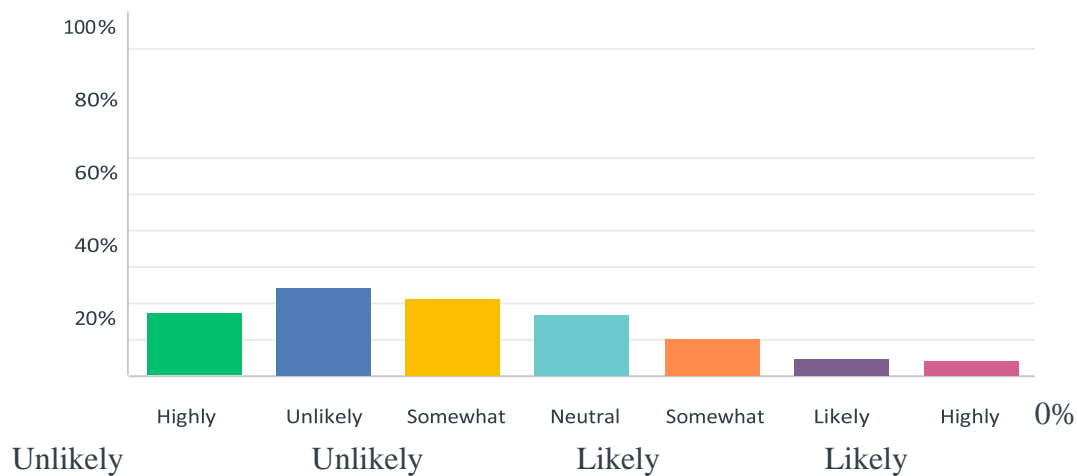
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES
Highly Unlikely	17.82% 67
Unlikely	22.34% 84
Somewhat Unlikely	16.49% 62
Neutral	16.76% 63
Somewhat Likely	12.50% 47
Likely	8.24% 31
Highly Likely	5.85% 22
TOTAL	376

Q21 My computer is downloading a virus or an application with many bugs.

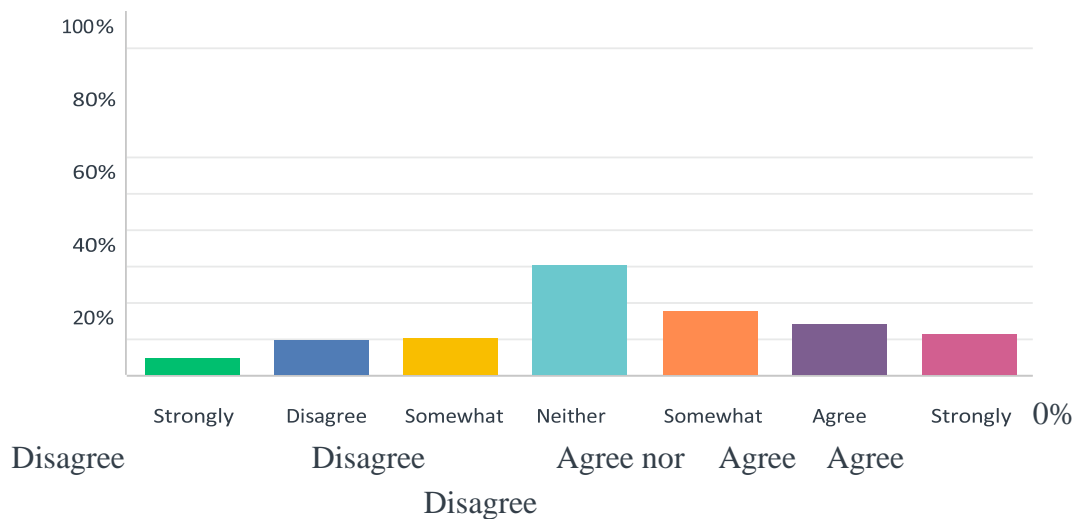
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Highly Unlikely	17.29%	65
Unlikely	24.47%	92
Somewhat Unlikely	21.28%	80
Neutral	16.76%	63
Somewhat Likely	10.64%	40
Likely	5.05%	19
Highly Likely	4.52%	17
TOTAL		376

Q22 Using anti-spyware software increases my productivity.

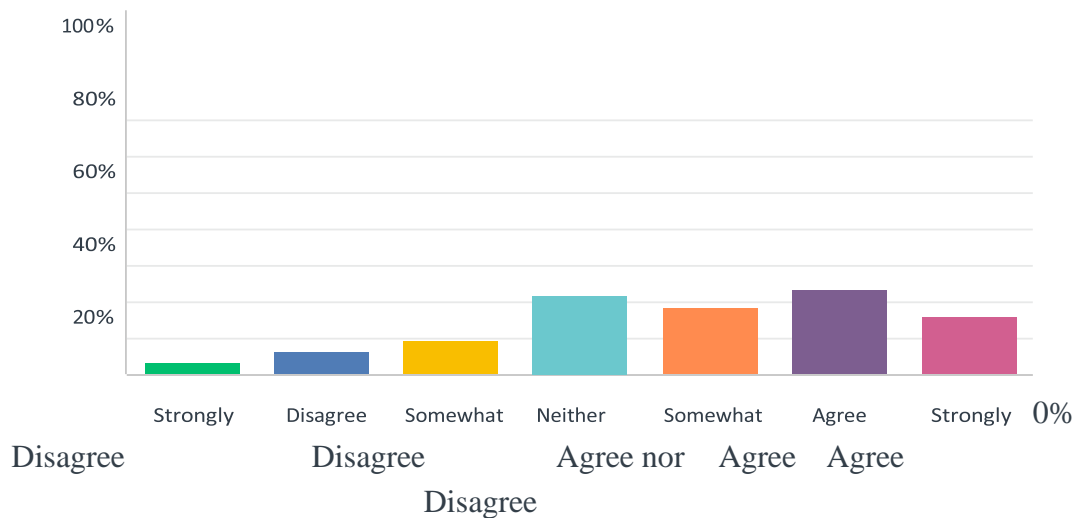
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	5.05%	19
Disagree	10.11%	38
Somewhat Disagree	10.64%	40
Neither Agree nor Disagree	30.32%	114
Somewhat Agree	17.82%	67
Agree	14.36%	54
Strongly Agree	11.70%	44
TOTAL		376

Q23 I am confident about selecting the appropriate security software to use on my computer.

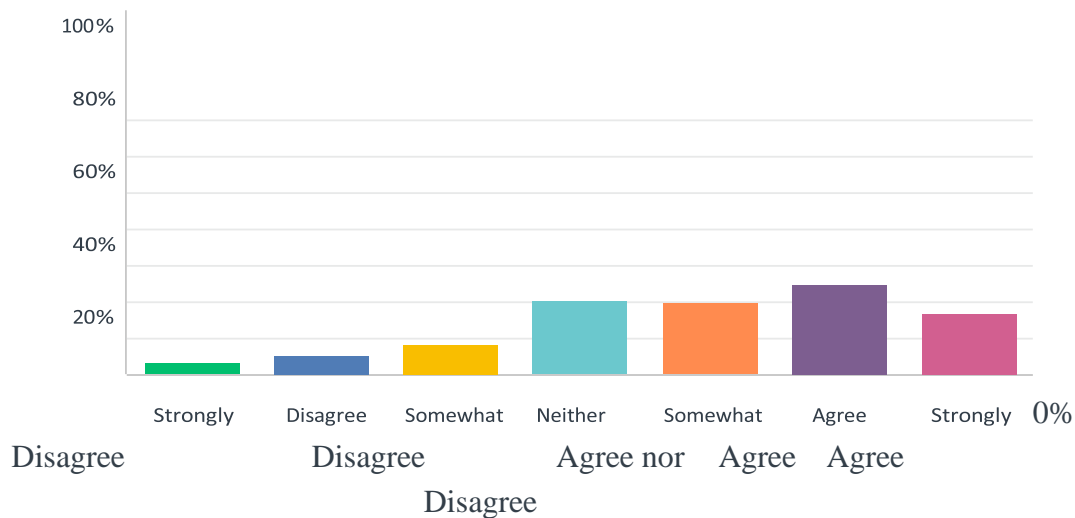
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	3.72%	14
Disagree	6.65%	25
Somewhat Disagree	9.31%	35
Neither Agree nor Disagree	22.07%	83
Somewhat Agree	18.62%	70
Agree	23.67%	89
Strongly Agree	15.96%	60
TOTAL		376

Q24 I am confident about selecting the appropriate security settings on my computer.

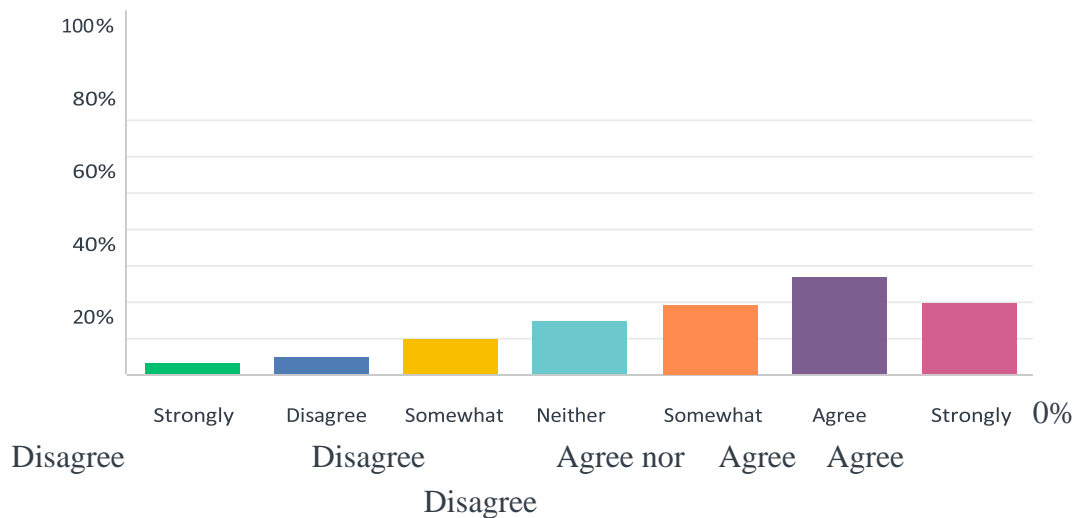
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	3.46%	13
Disagree	5.59%	21
Somewhat Disagree	8.51%	32
Neither Agree nor Disagree	20.74%	78
Somewhat Agree	19.95%	75
Agree	25.00%	94
Strongly Agree	16.76%	63
TOTAL		376

Q25 I am confident of correctly installing security software on my computer.

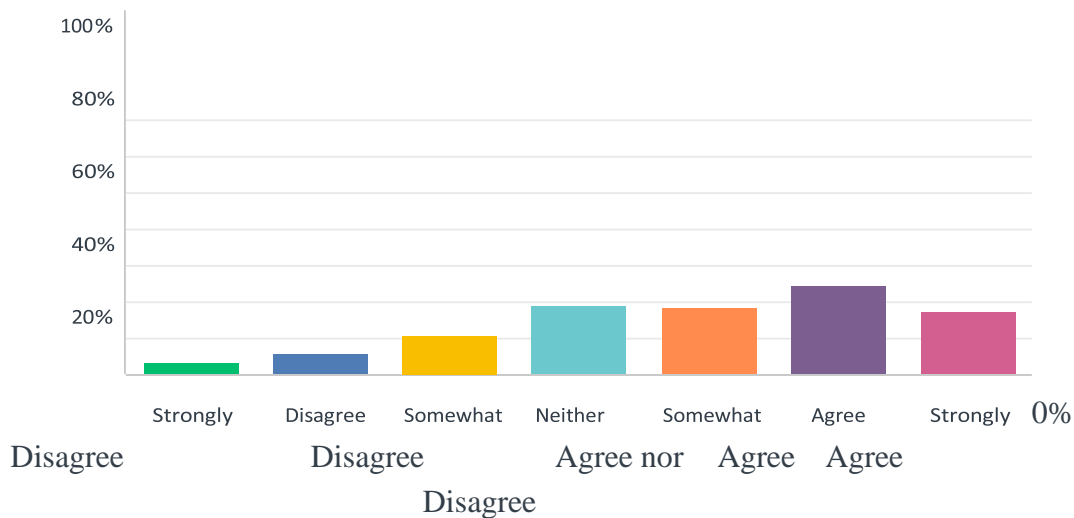
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	3.46%	13
Disagree	4.79%	18
Somewhat Disagree	10.11%	38
Neither Agree nor Disagree	14.89%	56
Somewhat Agree	19.68%	74
Agree	26.86%	101
Strongly Agree	20.21%	76
TOTAL		376

Q26 I am confident of quickly finding information on using security software on my computer.

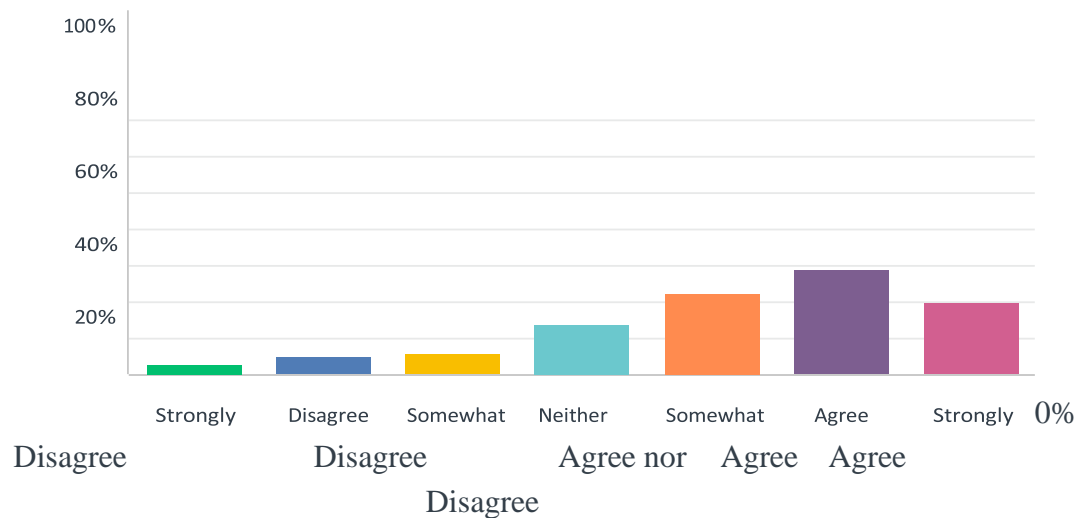
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	3.72%	14
Disagree	5.85%	22
Somewhat Disagree	11.17%	42
Neither Agree nor Disagree	18.88%	71
Somewhat Agree	18.35%	69
Agree	24.73%	93
Strongly Agree	17.29%	65
TOTAL		376

Q27 Using anti-virus software works to protect my computer from a data breach.

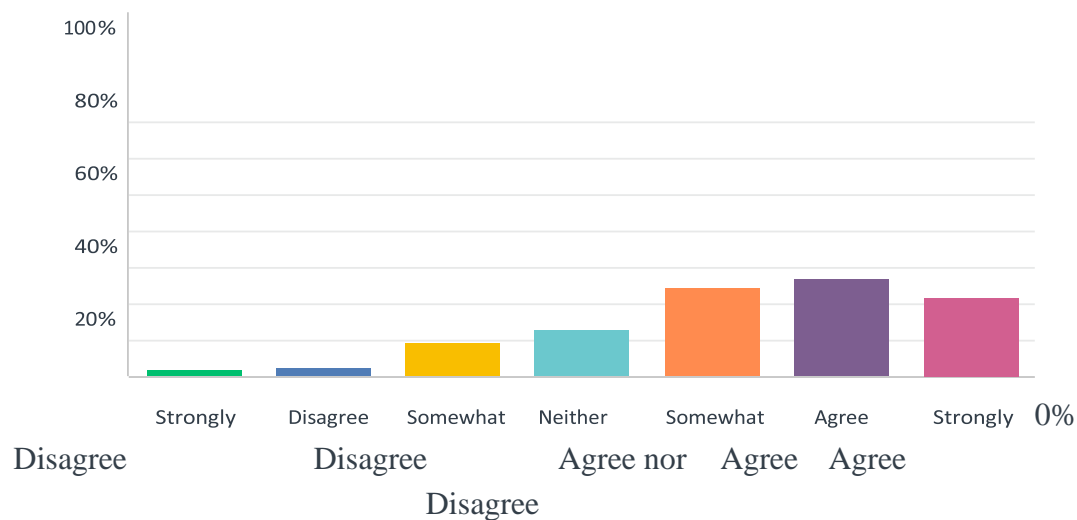
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	3.19%	12
Disagree	4.79%	18
Somewhat Disagree	6.12%	23
Neither Agree nor Disagree	14.10%	53
Somewhat Agree	22.61%	85
Agree	28.99%	109
Strongly Agree	20.21%	76
TOTAL		376

Q28 Using anti-malware software works to protect my computer from a data breach.

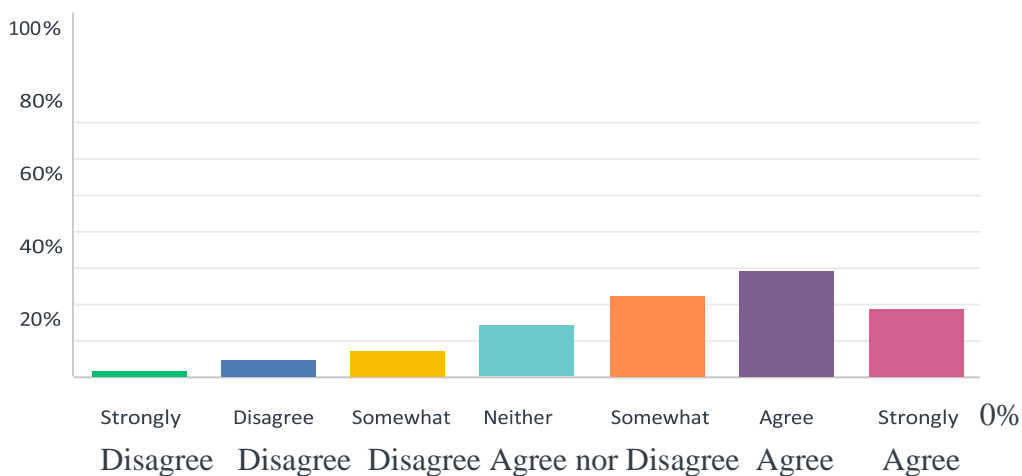
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	1.86%	7
Disagree	2.66%	10
Somewhat Disagree	9.31%	35
Neither Agree nor Disagree	12.77%	48
Somewhat Agree	24.47%	92
Agree	27.13%	102
Strongly Agree	21.81%	82
TOTAL		376

Q29 Using anti-virus software is effective in protecting my computer from a data breach.

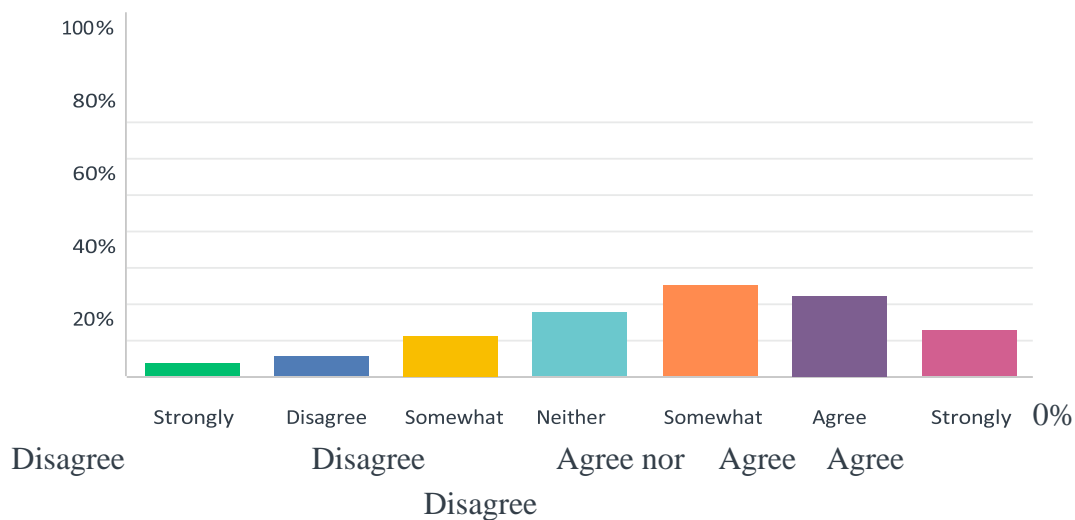
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES
Strongly Disagree	2.13% 8
Disagree	4.79% 18
Somewhat Disagree	7.71% 29
Neither Agree nor Disagree	14.63% 55
Somewhat Agree	22.34% 84
Agree	29.26% 110
Strongly Agree	19.15% 72
TOTAL	376

Q30 Using an anti-malware software is sufficient to protect my computer from a data breach.

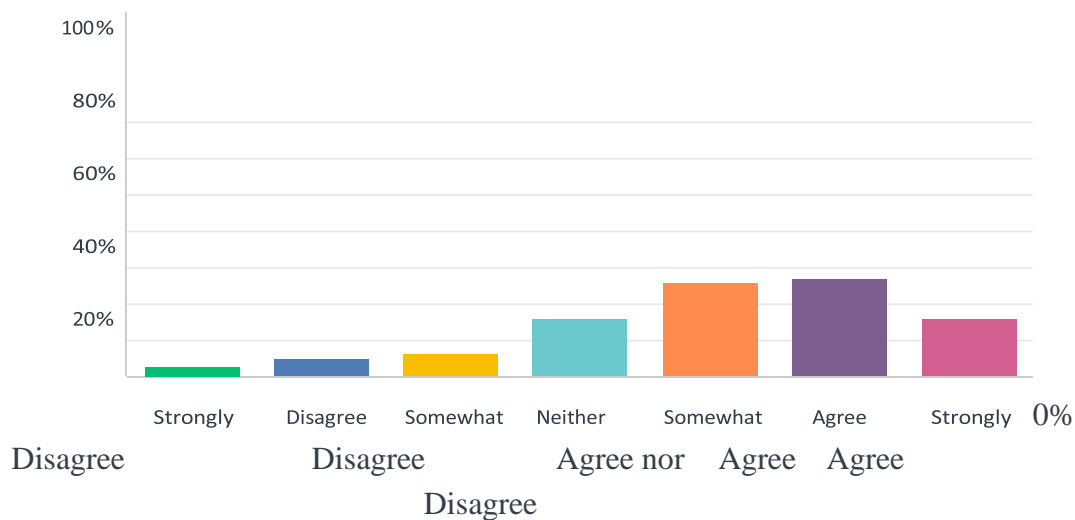
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	3.99%	15
Disagree	6.12%	23
Somewhat Disagree	11.44%	43
Neither Agree nor Disagree	17.82%	67
Somewhat Agree	25.27%	95
Agree	22.34%	84
Strongly Agree	13.03%	49
TOTAL		376

Q31 Using an anti-virus software would more likely protect my computer from a data breach.

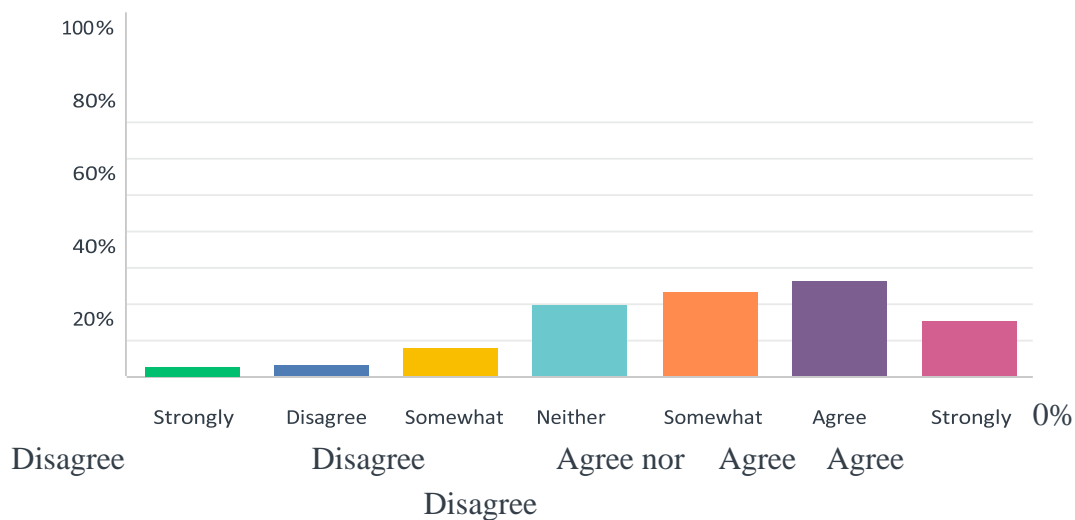
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES
Strongly Disagree	2.93% 11
Disagree	5.05% 19
Somewhat Disagree	6.65% 25
Neither Agree nor Disagree	15.96% 60
Somewhat Agree	26.06% 98
Agree	27.13% 102
Strongly Agree	16.22% 61
TOTAL	376

Q32 Using anti-malware software would more likely protect my computer from a data breach.

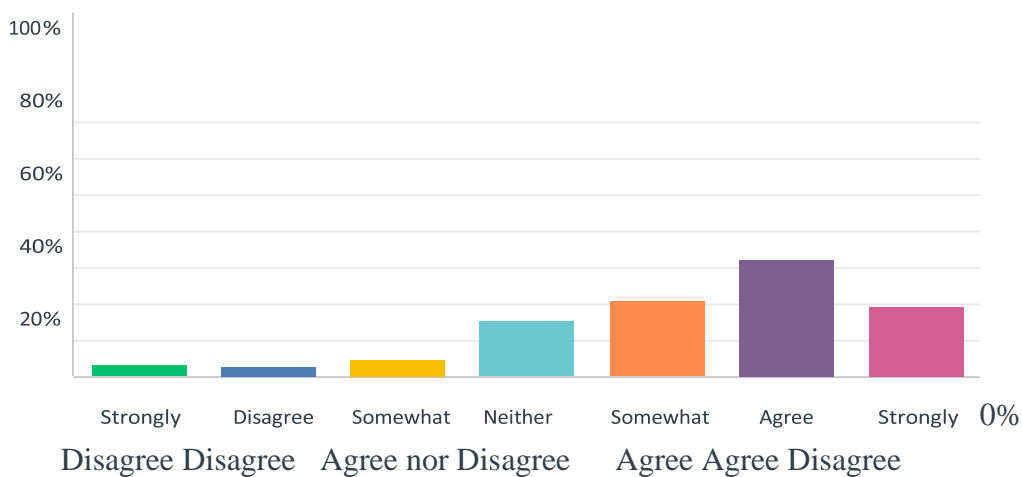
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES
Strongly Disagree	2.93% 11
Disagree	3.46% 13
Somewhat Disagree	7.98% 30
Neither Agree nor Disagree	20.21% 76
Somewhat Agree	23.40% 88
Agree	26.33% 99
Strongly Agree	15.69% 59
TOTAL	376

Q33 Installation and frequent updates of anti-virus software is effective in preventing virus infections on my computer.

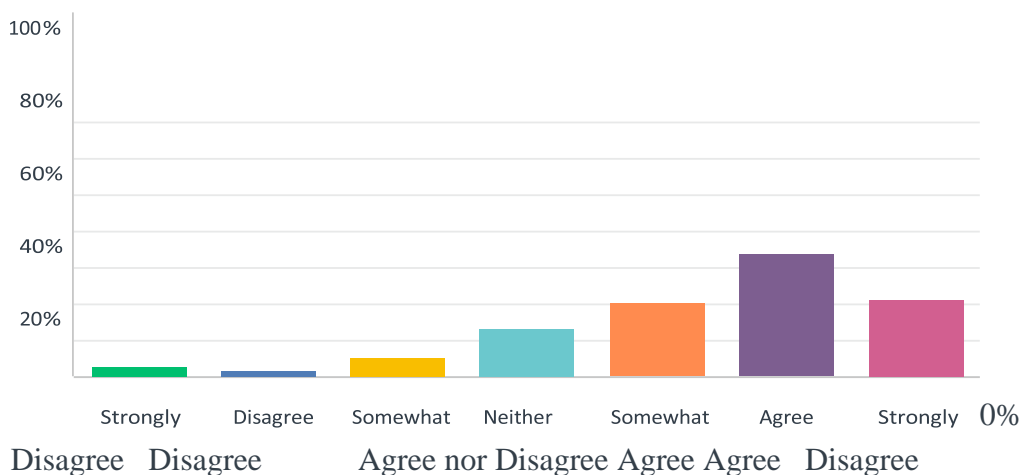
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	3.46%	13
Disagree	2.93%	11
Somewhat Disagree	5.05%	19
Neither Agree nor Disagree	15.43%	58
Somewhat Agree	21.01%	79
Agree	32.45%	122
Strongly Agree	19.68%	74
TOTAL		376

Q34 If I install anti-virus software on my computer and update it frequently, I am less likely to have my system infected by a virus.

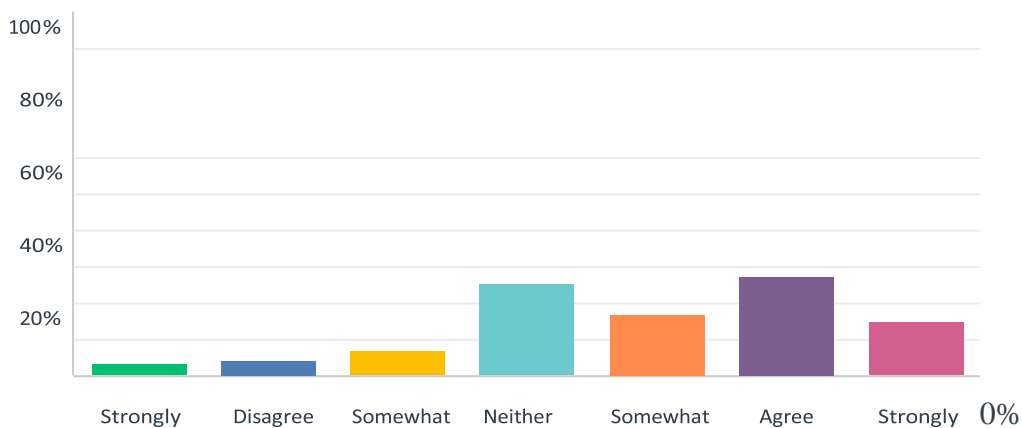
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	3.19%	12
Disagree	1.86%	7
Somewhat Disagree	5.32%	20
Neither Agree nor Disagree	13.56%	51
Somewhat Agree	20.48%	77
Agree	34.04%	128
Strongly Agree	21.54%	81
TOTAL		376

Q35 I find the use of anti-spyware software useful in my job.

Answered: 376 Skipped: 0

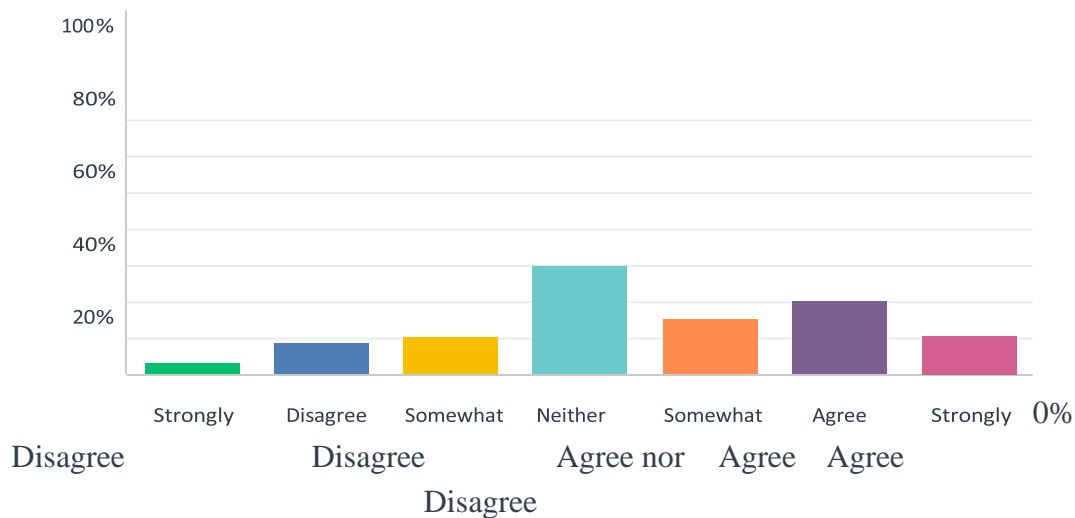


Disagree Disagree Agree nor Agree Agree
Disagree

ANSWER CHOICES	RESPONSES
Strongly Disagree	3.72% 14
Disagree	4.26% 16
Somewhat Disagree	7.18% 27
Neither Agree nor Disagree	25.53% 96
Somewhat Agree	16.76% 63
Agree	27.66% 104
Strongly Agree	14.89% 56
TOTAL	376

Q36 Using anti-spyware software enables me to accomplish tasks more quickly.

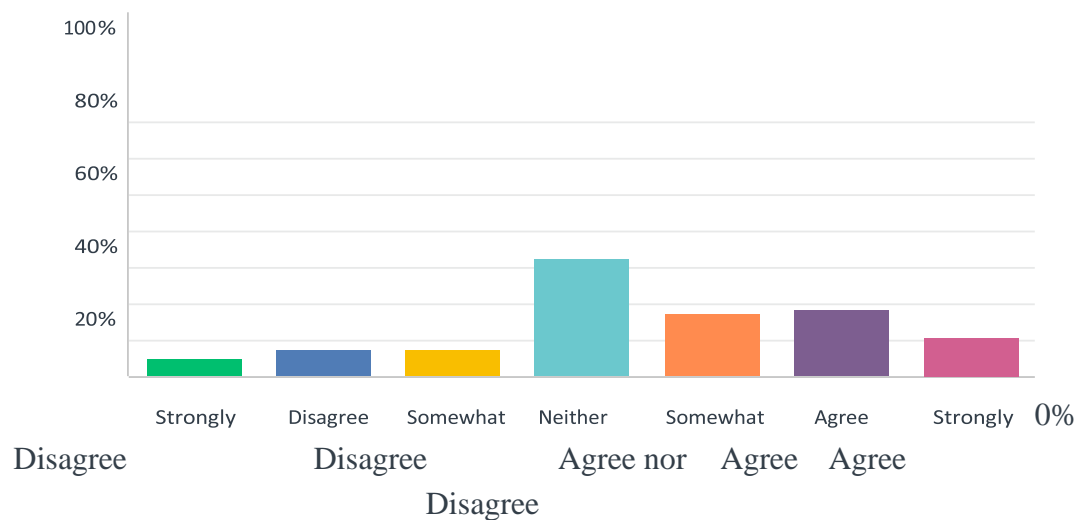
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	3.46%	13
Disagree	9.04%	34
Somewhat Disagree	10.37%	39
Neither Agree nor Disagree	30.05%	113
Somewhat Agree	15.43%	58
Agree	20.48%	77
Strongly Agree	11.17%	42
TOTAL		376

Q37 People who influence my behavior think that I should use antispyware software.

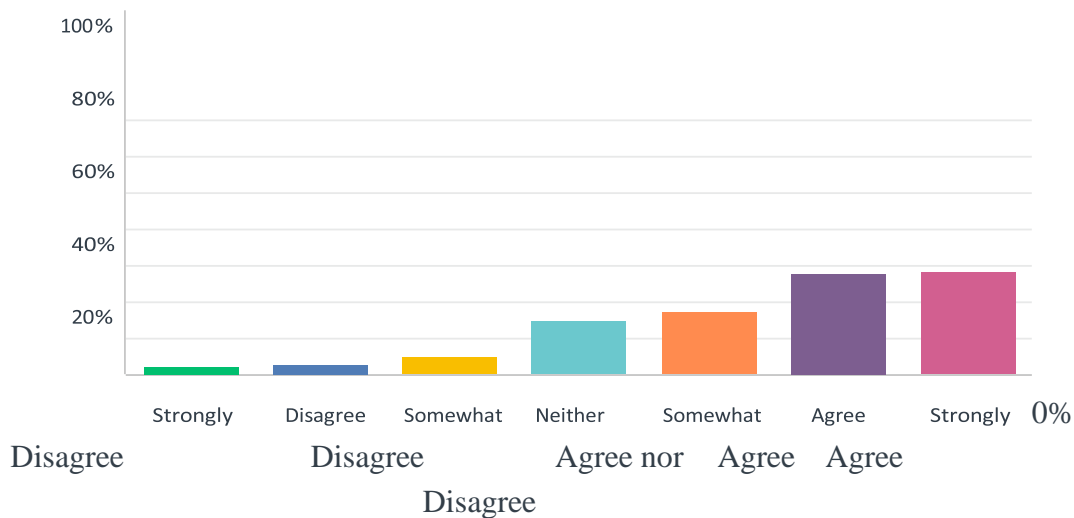
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES
Strongly Disagree	5.05% 19
Disagree	7.71% 29
Somewhat Disagree	7.45% 28
Neither Agree nor Disagree	32.45% 122
Somewhat Agree	17.55% 66
Agree	18.62% 70
Strongly Agree	11.17% 42
TOTAL	376

Q38 In general, my organization has supported using and providing antispymware software.

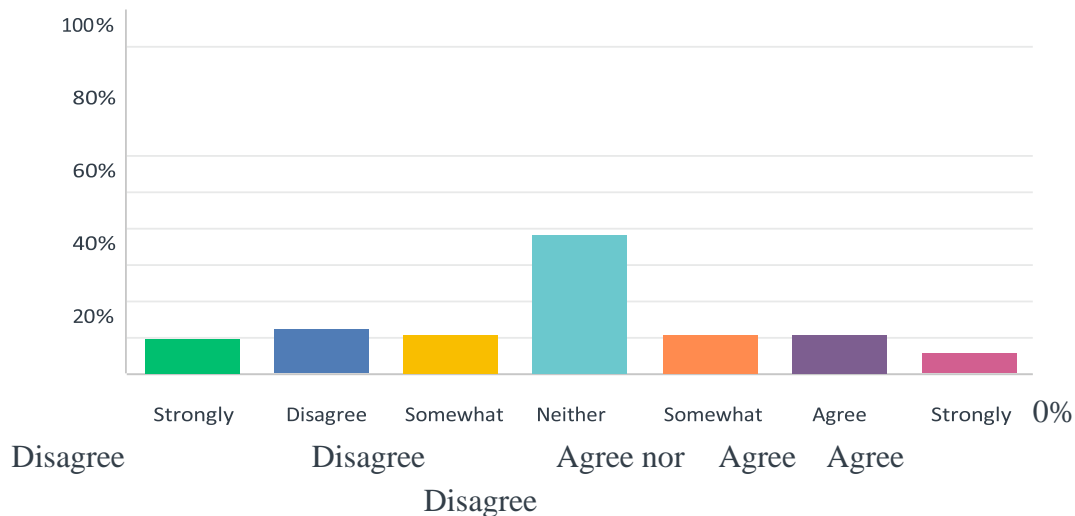
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	2.66%	10
Disagree	3.19%	12
Somewhat Disagree	5.05%	19
Neither Agree nor Disagree	15.16%	57
Somewhat Agree	17.55%	66
Agree	27.93%	105
Strongly Agree	28.46%	107
TOTAL		376

Q39 Anti-spyware software makes work more interesting.

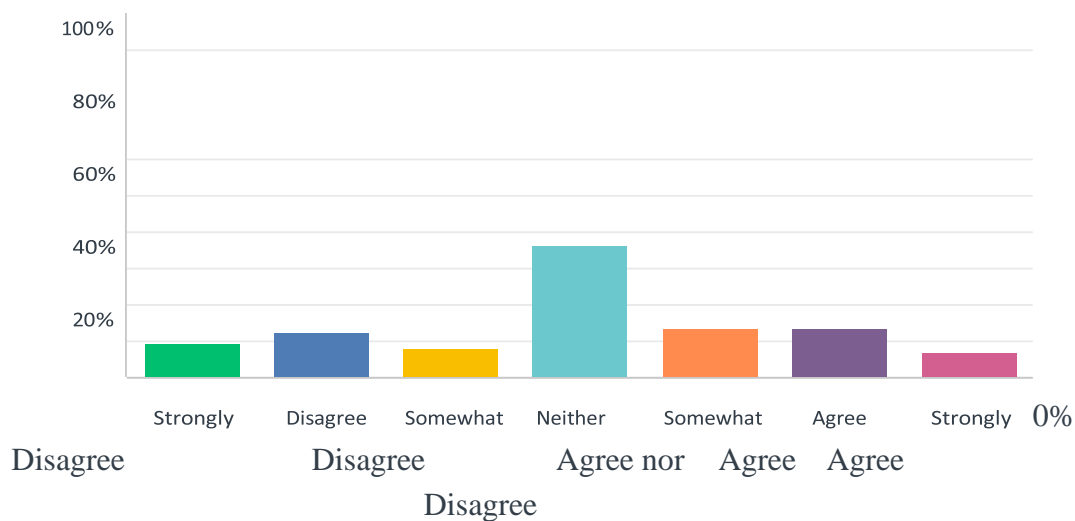
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	10.11%	38
Disagree	12.50%	47
Somewhat Disagree	11.17%	42
Neither Agree nor Disagree	38.30%	144
Somewhat Agree	10.90%	41
Agree	11.17%	42
Strongly Agree	5.85%	22
TOTAL		376

Q40 Working with anti-spyware software is fun.

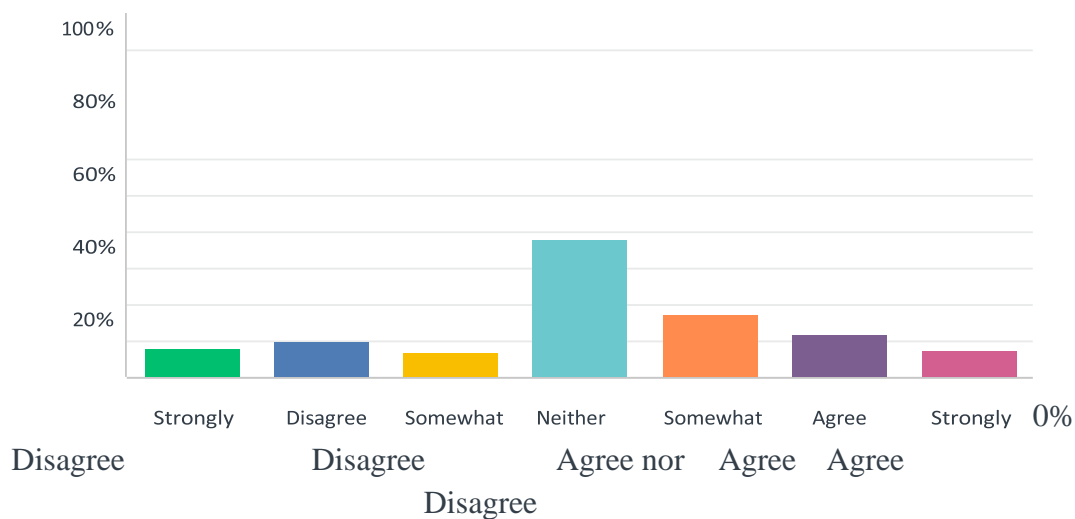
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	9.57%	36
Disagree	12.50%	47
Somewhat Disagree	7.98%	30
Neither Agree nor Disagree	36.44%	137
Somewhat Agree	13.30%	50
Agree	13.30%	50
Strongly Agree	6.91%	26
TOTAL		376

Q 41 I like working with anti-spyware software.

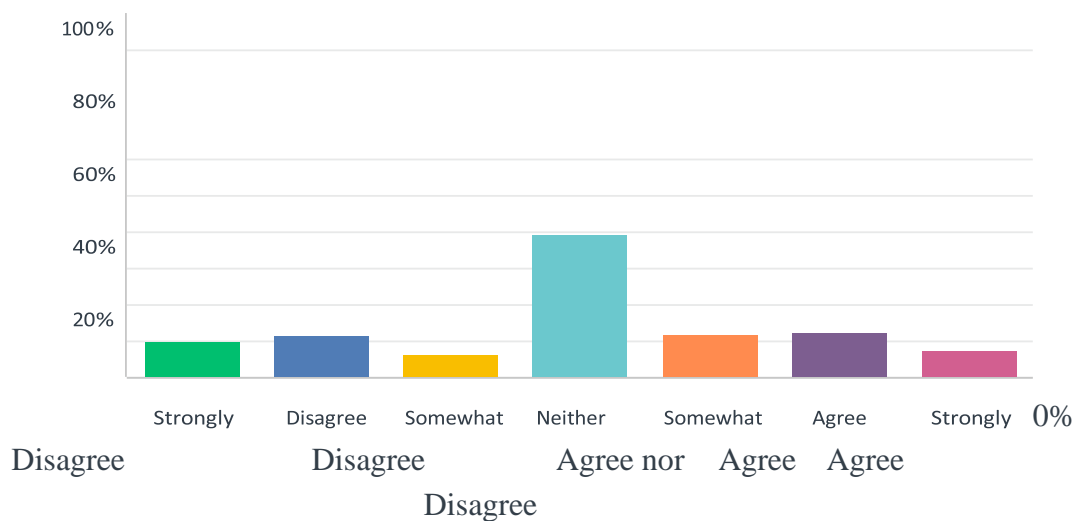
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	8.24%	31
Disagree	9.84%	37
Somewhat Disagree	6.91%	26
Neither Agree nor Disagree	37.77%	142
Somewhat Agree	17.55%	66
Agree	12.23%	46
Strongly Agree	7.45%	28
TOTAL		376

Q42 Working with anti-spyware software is enjoyable.

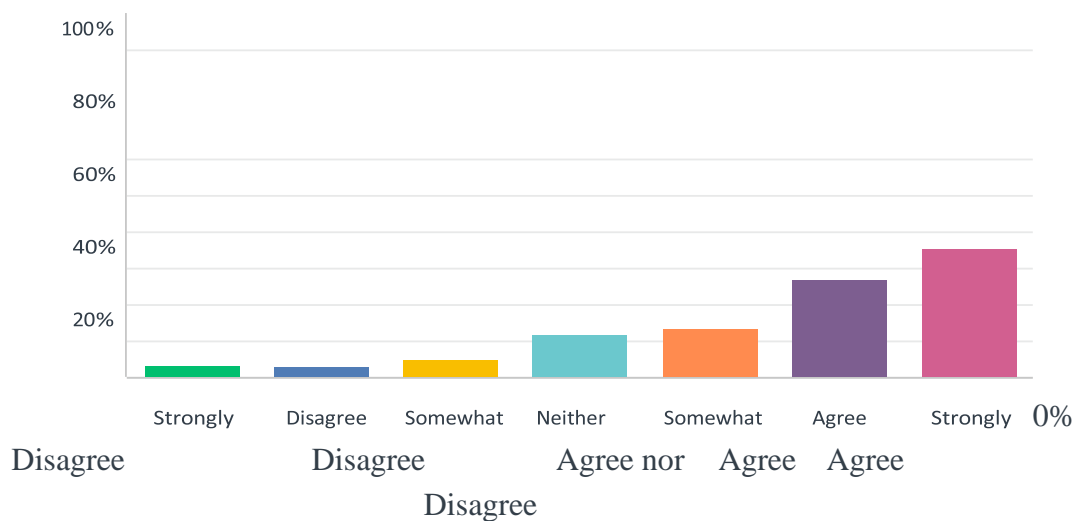
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	9.84%	37
Disagree	11.70%	44
Somewhat Disagree	6.65%	25
Neither Agree nor Disagree	39.63%	149
Somewhat Agree	12.23%	46
Agree	12.50%	47
Strongly Agree	7.45%	28
TOTAL		376

Q43 I am motivated to protect my computer from threats of a data breach.

Answered: 376 Skipped: 0

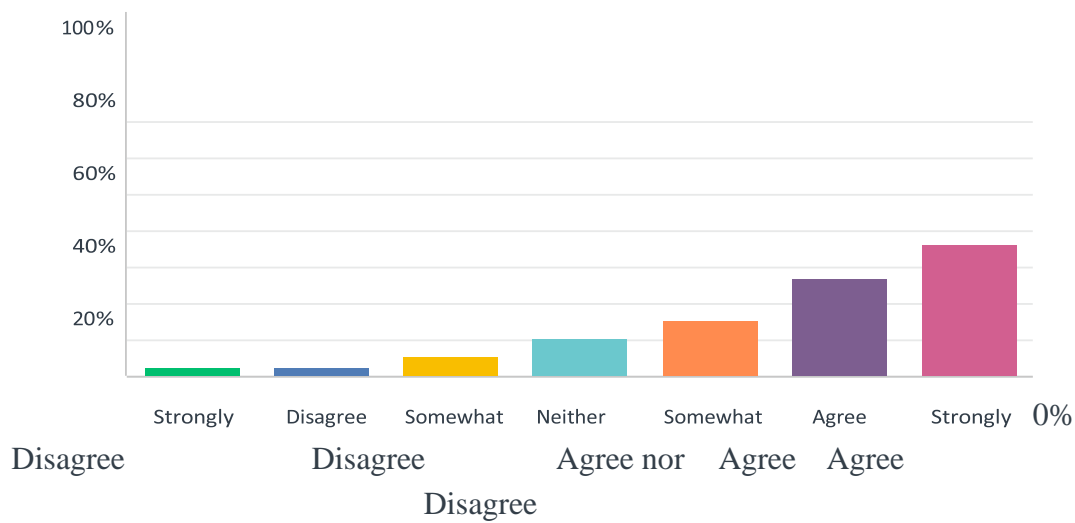


ANSWER CHOICES	RESPONSES	
Strongly Disagree	3.72%	14
Disagree	2.93%	11
Somewhat Disagree	5.05%	19
Neither Agree nor Disagree	12.23%	46
Somewhat Agree	13.56%	51
Agree	26.86%	101
Strongly Agree	35.64%	134
TOTAL		376

Q44 I am motivated to prevent threats a data breach to my computer from being successful

ANSWER CHOICES	RESPONSES
Strongly Disagree	2.66% 10
Disagree	2.39% 9
Somewhat Disagree	5.32% 20
Neither Agree nor Disagree	10.64% 40
Somewhat Agree	15.43% 58
Agree	27.13% 102
Strongly Agree	36.44% 137
TOTAL	376

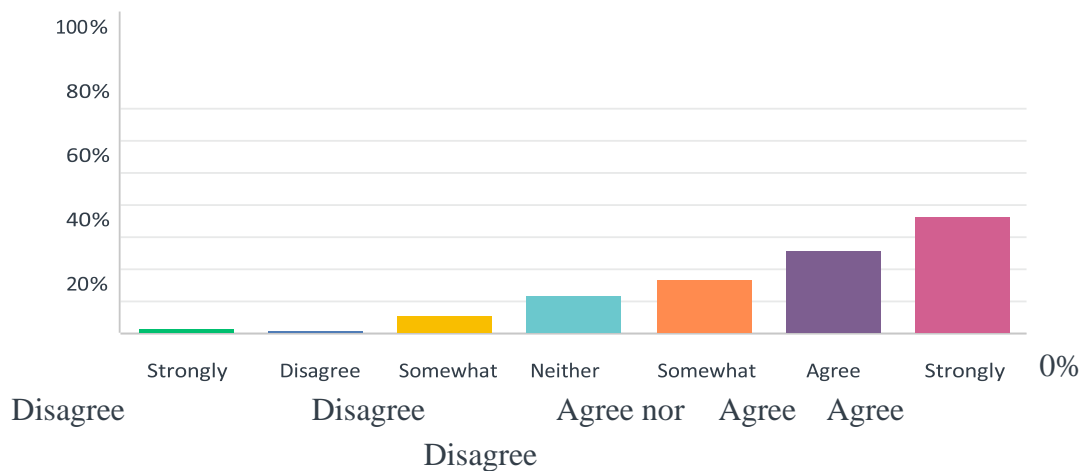
Answered: 376 Skipped: 0



Q45 I am motivated to engage in activities that protect my computer from threats of a data breach.

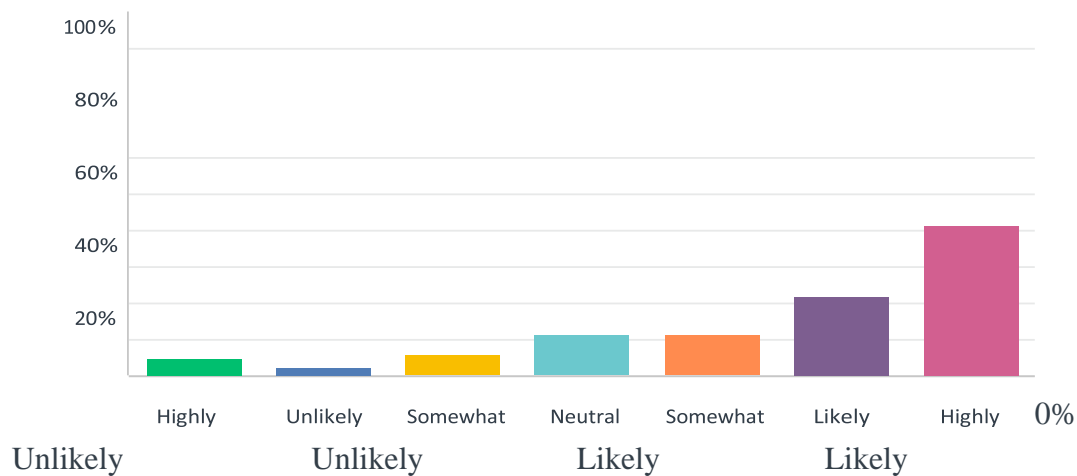
ANSWER CHOICES	RESPONSES
Strongly Disagree	1.60% 6
Disagree	1.06% 4
Somewhat Disagree	5.59% 21
Neither Agree nor Disagree	11.97% 45
Somewhat Agree	17.02% 64
Agree	26.06% 98
Strongly Agree	36.70% 138
TOTAL	376

Answered: 376 Skipped: 0



Q 46 I use firewall protection on my computer.

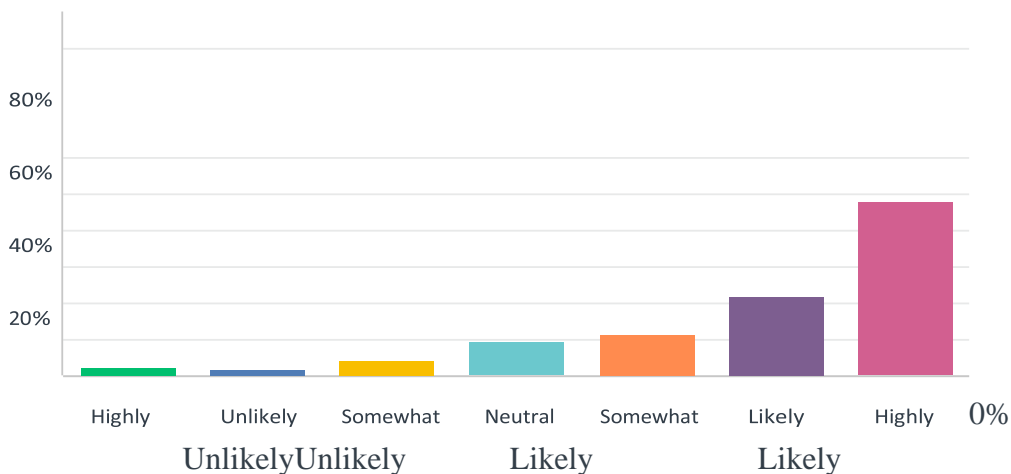
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Highly Unlikely	4.79%	18
Unlikely	2.66%	10
Somewhat Unlikely	6.12%	23
Neutral	11.44%	43
Somewhat Likely	11.44%	43
Likely	22.07%	83
Highly Likely	41.49%	156
TOTAL		376

Q47 I use anti-virus software on my computer.

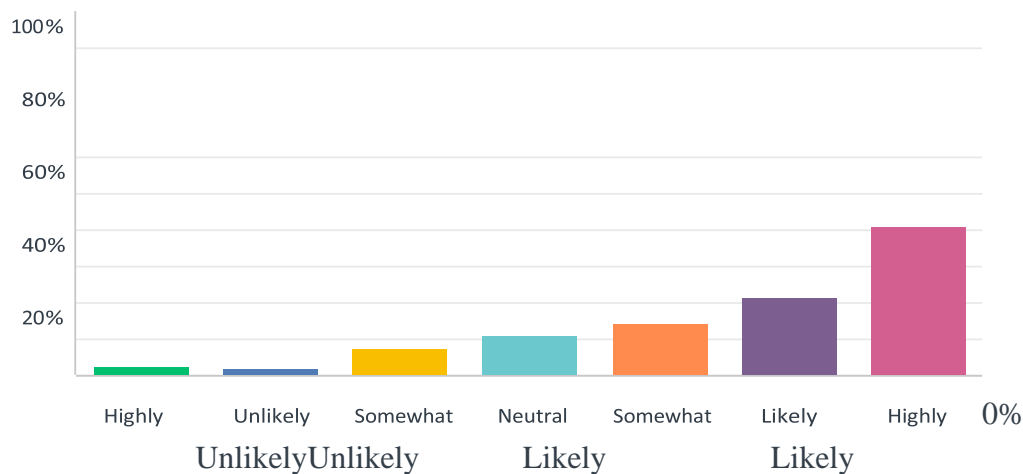
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Highly Unlikely	2.39%	9
Unlikely	2.13%	8
Somewhat Unlikely	4.26%	16
Neutral	9.57%	36
Somewhat Likely	11.70%	44
Likely	21.81%	82
Highly Likely	48.14%	181
TOTAL		376

Q48 I use anti-malware software on my computer.

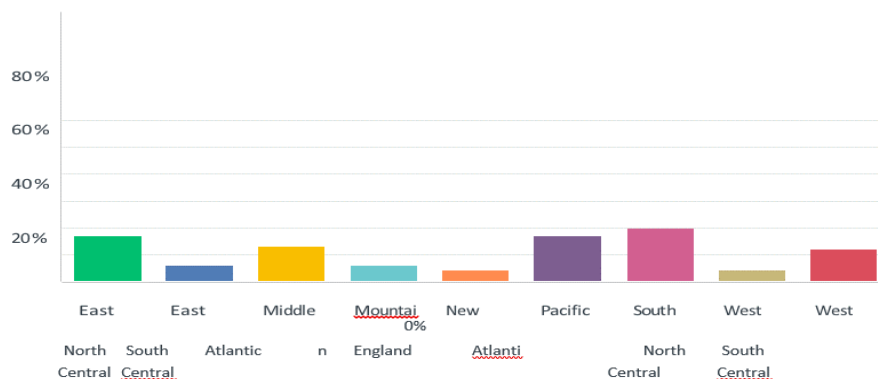
Answered: 376 Skipped: 0



ANSWER CHOICES	RESPONSES	
Highly Unlikely	2.39%	9
Unlikely	2.13%	8
Somewhat Unlikely	7.45%	28
Neutral	10.90%	41
Somewhat Likely	14.63%	55
Likely	21.28%	80
Highly Likely	41.22%	155
TOTAL		376

Q49 Region

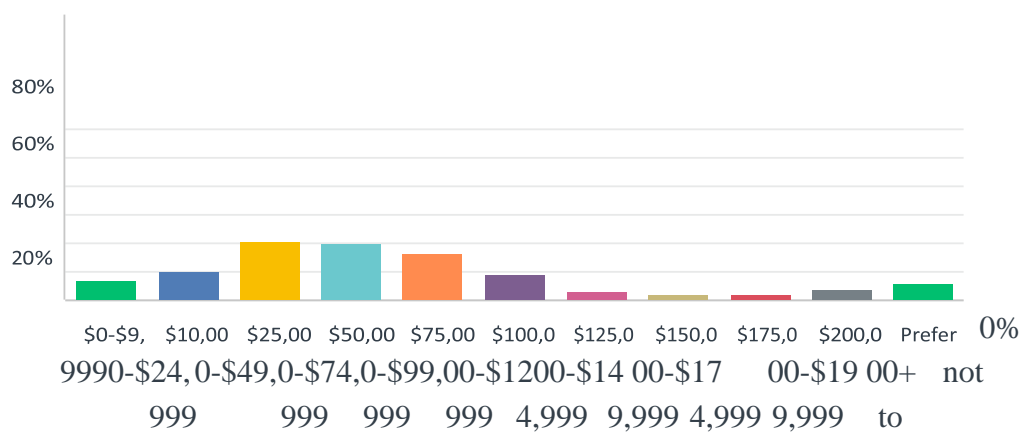
Answered: 368 Skipped: 8



ANSWER CHOICES	RESPONSES	
East North Central	16.85%	62
East South Central	6.25%	23
Middle Atlantic	13.04%	48
Mountain	5.98%	22
New England	4.35%	16
Pacific	17.12%	63
South Atlantic	19.84%	73
West North Central	4.62%	17
West South Central	11.96%	44
TOTAL		368

Q50 Household Income

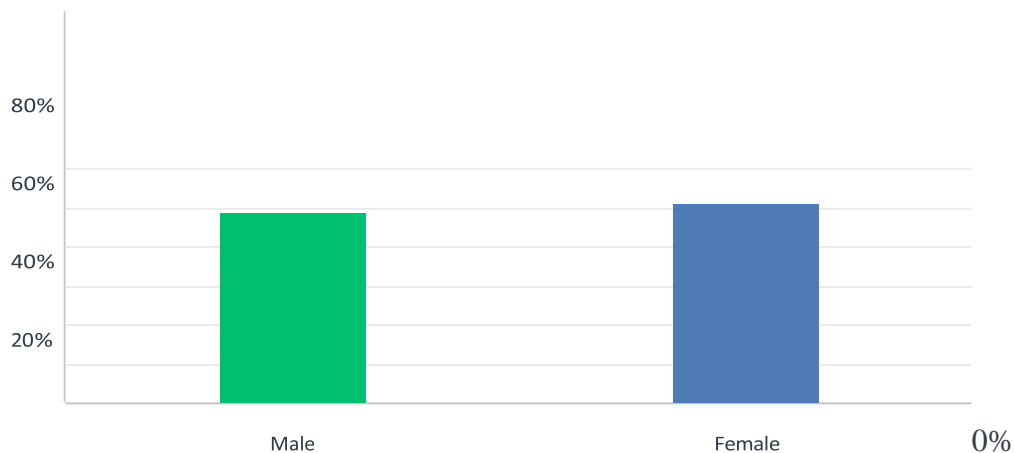
Answered: 373 Skipped: 3



ANSWER CHOICES	RESPONSES	
\$0-\$9,999	7.24%	27
\$10,000-\$24,999	10.19%	38
\$25,000-\$49,999	20.38%	76
\$50,000-\$74,999	19.84%	74
\$75,000-\$99,999	16.35%	61
\$100,000-\$124,999	8.85%	33
\$125,000-\$149,999	3.22%	12
\$150,000-\$174,999	2.14%	8
\$175,000-\$199,999	1.88%	7
\$200,000+	4.02%	15
Prefer not to answer	5.90%	22
TOTAL		373

Q51 Gender

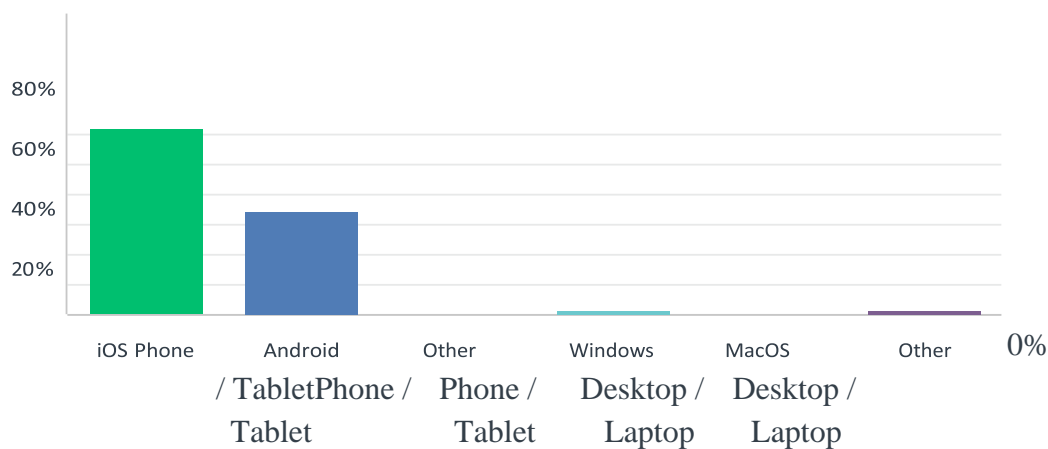
Answered: 373 Skipped: 3



ANSWER CHOICES	RESPONSES	
Male	49.06%	183
Female	50.94%	190
TOTAL		373

Q52 Device Type

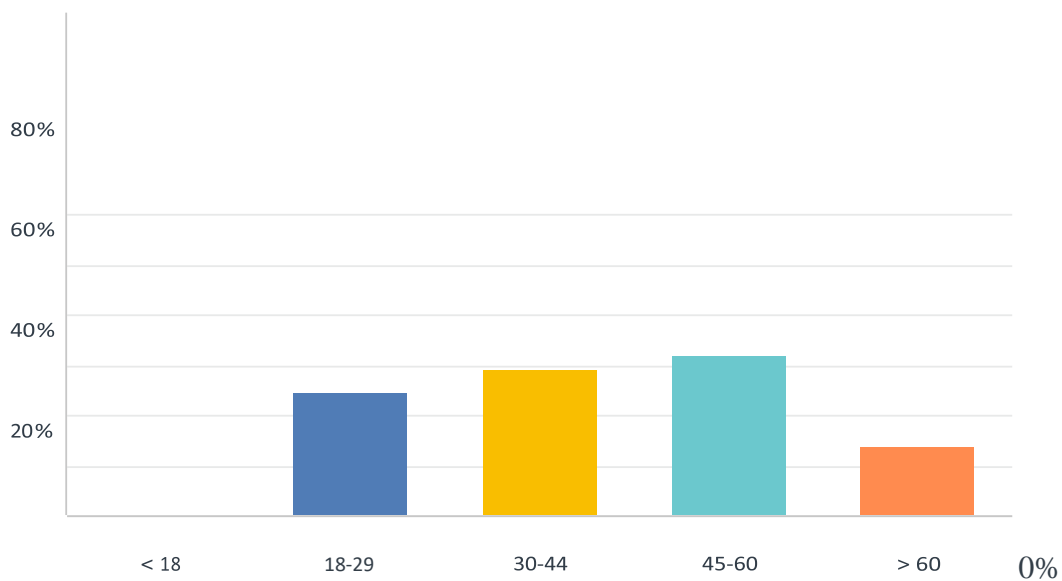
Answered: 373 Skipped: 3



ANSWER CHOICES	RESPONSES	
iOS Phone / Tablet	62.20%	232
Android Phone / Tablet	34.58%	129
Other Phone / Tablet	0.00%	0
Windows Desktop / Laptop	1.34%	5
MacOS Desktop / Laptop	0.54%	2
Other	1.34%	5
TOTAL		373

Q53 Age

Answered: 373 Skipped: 3



ANSWER CHOICES	RESPONSES	
< 18	0.00%	0
18-29	24.66%	92
30-44	29.22%	109
45-60	32.17%	120
> 60	13.94%	52
TOTAL		373

Appendix C:

Mahalanobis Distance and Stem & Leaf Plot

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Mahalanobis Distance	376	100.0%	0	0.0%	376	100.0%

Descriptives

		Statistic	Std. Error	
Mahalanobis Distance	Mean	9.0000	.34816	
	95% Confidence Interval for Mean	Lower Bound	8.3154	
		Upper Bound	9.6846	
	5% Trimmed Mean	8.2701		
	Median	7.1708		
	Variance	45.578		
	Std. Deviation	6.75114		
	Minimum	.11		
	Maximum	74.65		
	Range	74.54		
	Interquartile Range	6.35		
	Skewness	3.602	.126	
	Kurtosis	25.392	.251	

M-Estimators

	Huber's M- Estimator ^a	Tukey's Biweight ^b	Hampel's M- Estimator ^c	Andrews' Wave ^d
Mahalanobis Distance	7.6257	7.1528	7.5923	7.1459

a. The weighting constant is 1.339.

- b. The weighting constant is 4.685.
 c. The weighting constants are 1.700, 3.400, and 8.500
 d. The weighting constant is $1.340 \cdot \pi$.

Percentiles

		Percentiles			
		5	10	25	50
Weighted Average(Definition 1)	Mahalanobis Distance	2.8040	3.6257	4.8956	7.1708
Tukey's Hinges	Mahalanobis Distance			4.9000	7.1708

Percentiles

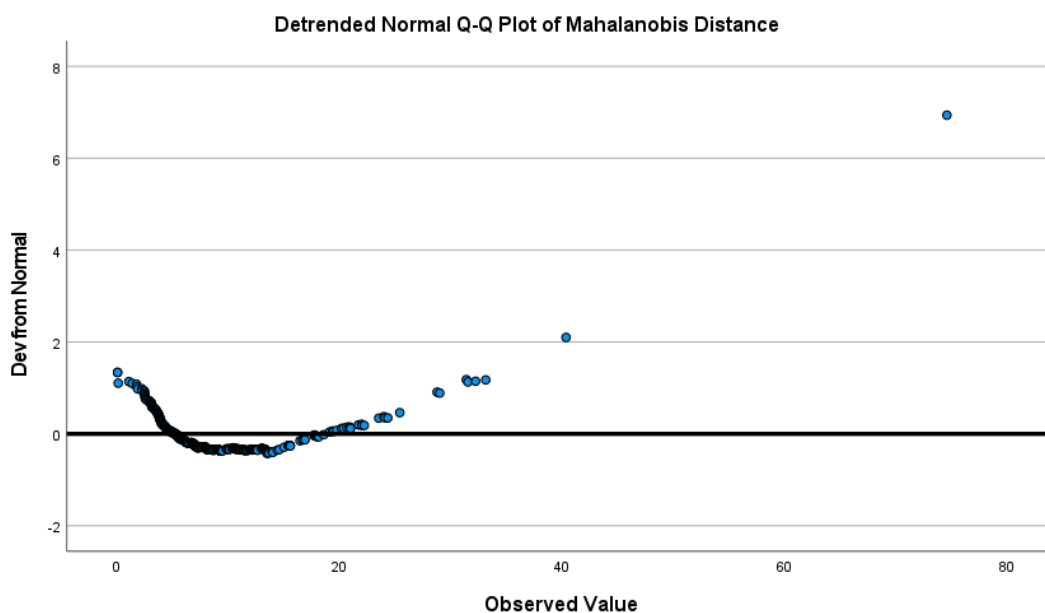
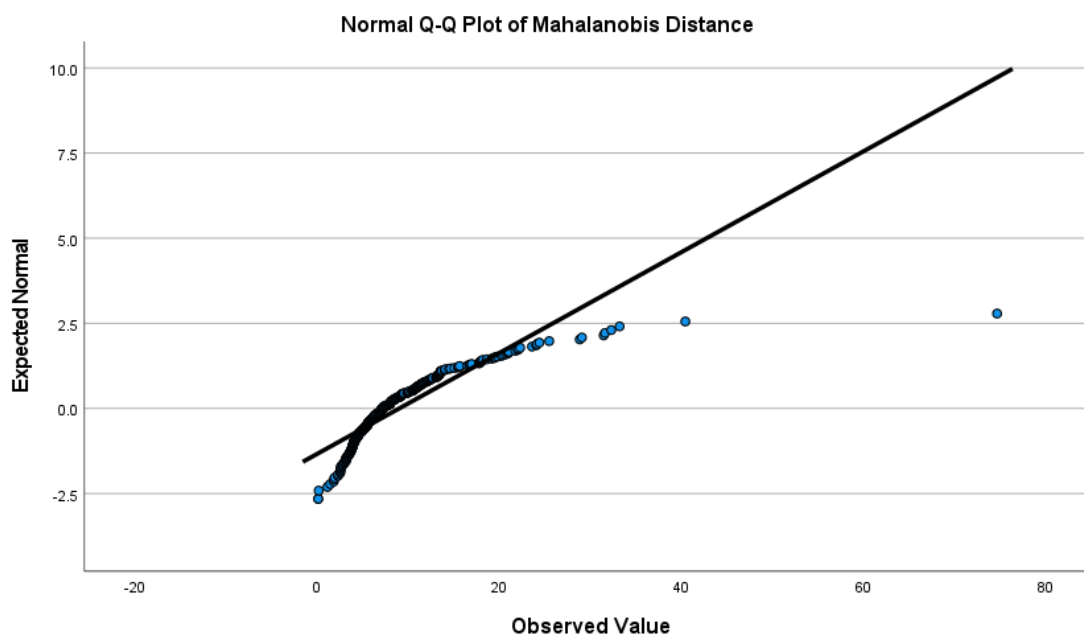
		Percentiles		
		75	90	95
Weighted Average(Definition 1)	Mahalanobis Distance	11.2480	16.7709	21.0315
Tukey's Hinges	Mahalanobis Distance	11.2163		

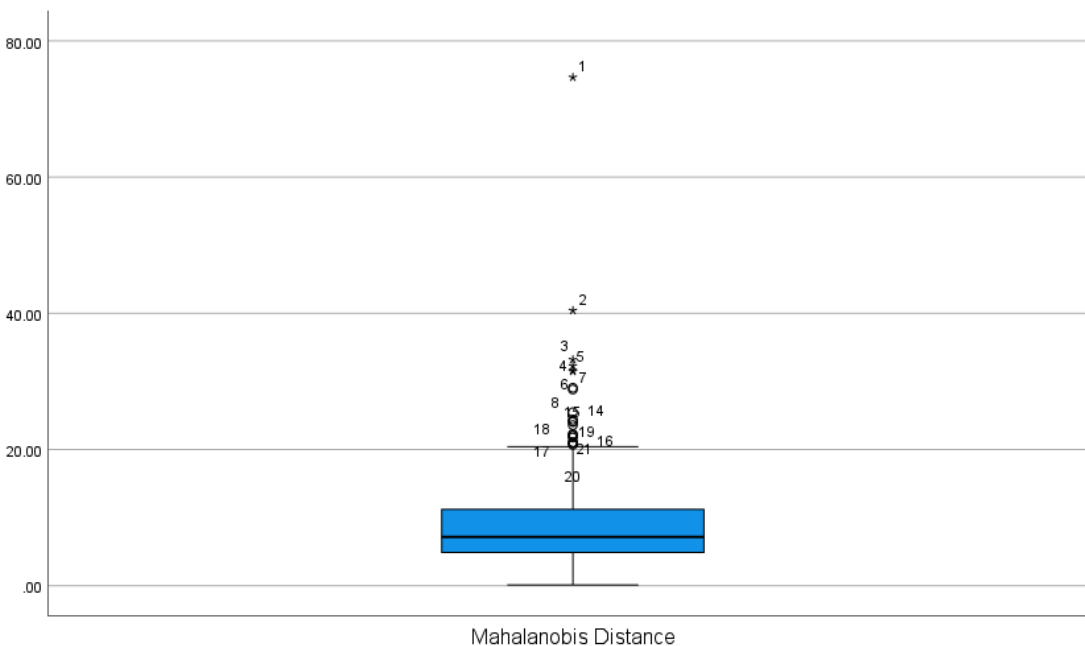
Extreme Values

		Case Number	Value	
Mahalanobis Distance	Highest	1	74.65	
		2	40.42	
		3	33.21	
		4	32.29	
		5	31.61	
	Lowest	1	376	.11
		2	375	.11
		3	374	.17
		4	373	1.13
		5	372	1.43

8.00 1 . 66667777
 8.00 1 . 88889999
 2.00 2 . 00
 21.00 Extremes (>=21)

Stem width: 10.00
 Each leaf: 1 case(s)





TSE	TSU	SEF	RES	PER	SIN	AT	CS	Mahalanobi	pMAH_	
V	S	F	P	F	F	T	PM	s Distance	1	
							1.0			
2.00	1.00	7.00	6.13	7.00	7.00	1.00	0	7.00	74.65	0.0000
							7.0			
1.00	1.00	1.00	0.88	2.50	2.50	1.00	0	7.00	40.42	0.0000
							4.0			
7.00	1.00	1.80	5.75	7.00	5.50	2.25	0	6.33	33.21	0.0001
							2.0			
4.17	2.63	3.00	4.50	6.00	4.00	4.00	0	6.67	32.29	0.0002
							6.0			
1.67	4.00	5.00	3.88	6.00	2.00	5.00	0	2.00	31.61	0.0002
							7.0			
2.50	1.00	4.20	1.25	2.00	5.00	3.75	0	6.00	31.46	0.0002
							1.6			
2.00	1.88	3.80	4.88	3.50	1.50	5.25	7	1.00	29.07	0.0006
							7.0			
1.50	3.38	5.80	2.50	6.00	6.00	4.25	0	7.00	28.83	0.0007

Appendix D:

A rerun of Mahalanobis Distance and Stem & Leaf Plot after eight extreme values deleted

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Mahalanobis Distance	366	100.0%	0	0.0%	366	100.0%

Descriptives

		Statistic	Std. Error	
Mahalanobis Distance	Mean	7.8841467	.24450379	
	95% Confidence Interval for Mean	Lower Bound	7.4033338	
		Upper Bound	8.3649596	
		5% Trimmed Mean	7.5338882	
	Median	6.6490169		
	Variance	21.880		
	Std. Deviation	4.67763284		
	Minimum	1.27656		
	Maximum	23.79373		
	Range	22.51717		
	Interquartile Range	5.92802		
	Skewness	1.090	.128	
	Kurtosis	.997	.254	

Descriptives		Bootstrap	
		Bias	Std. Error
Mahalanobis Distance	Mean	.0031793	.2451414
	95% Confidence Interval for Mean	Lower Bound	
		Upper Bound	
	5% Trimmed Mean	.0045843	.2514799
	Median	.0738553	.2405280
	Variance	-.017	1.968
	Std. Deviation	-.00657380	.21041903
	Minimum		
	Maximum		
	Range		
	Interquartile Range	.00773	.37929
	Skewness	-.010	.109
	Kurtosis	-.018	.379

Descriptives		Bootstrap	
		95% Confidence Interval	
		Lower	Upper
Mahalanobis Distance	Mean	7.4198598	8.3765648
	95% Confidence Interval for Mean	Lower Bound	
		Upper Bound	
	5% Trimmed Mean	7.0672694	8.0357909
	Median	6.3201370	7.2600308
	Variance	18.214	25.903
	Std. Deviation	4.26779998	5.08952903
	Minimum		
	Maximum		
	Range		
	Interquartile Range	5.22522	6.74240
	Skewness	.877	1.289
	Kurtosis	.313	1.727

a. Unless otherwise noted, bootstrap results are based on 500 bootstrap samples

M-Estimators

		Statistic	Bias	Bootstrap	
				Std. Error	95% Confidence Interval Lower
Mahalanobis Distance	Huber's M-Estimator ^a	7.1281770	.0061334	.2523725	6.6508723
	Tukey's Biweight ^b	6.7882698	.0109867	.2643190	6.2859469
	Hampel's M- Estimator ^c	7.1828120	-.0030839	.2581178	6.6662292
	Andrews' Wave ^d	6.7800764	.0082591	.2656301	6.2661631

M-Estimators

		Bootstrap 95% Confidence Interval Upper	
Mahalanobis Distance	Huber's M-Estimator ^a	7.6212882	
	Tukey's Biweight ^b	7.3056385	
	Hampel's M-Estimator ^c	7.6771322	
	Andrews' Wave ^d	7.2997380	

- a. The weighting constant is 1.339.
- b. The weighting constant is 4.685.
- c. The weighting constants are 1.700, 3.400, and 8.500
- d. The weighting constant is $1.340 \cdot \pi$.
- e. Unless otherwise noted, bootstrap results are based on 500 bootstrap samples

Percentiles

		Bootstrap			
		Percentiles	Percentile	Bias	Std. Error
Weighted Average(Definition 1)	Mahalanobis Distance	5	2.0943608	.0127229	.1047017
		10	2.8019423	-.0271455	.2116592
		25	4.4235371	.0066994	.2353941
		50	6.6490169	.0738553	.2405280
		75	10.3515546	.0144261	.3895981
		90	14.0689597	.1519868	.9405778
		95	17.6162341	.1110793	.5909047
Tukey's Hinges	Mahalanobis Distance	25	4.4298690	.0072805	.2369853
		50	6.6490169	.0738553	.2405280
		75	10.3509352	.0045292	.3879297

Percentiles

		Bootstrap		
		95% Confidence Interval		
		Percentiles	Lower	Upper
Weighted Average(Definition 1)	Mahalanobis Distance	5	1.8730229	2.4053100
		10	2.3533776	3.2136534
		25	4.0439209	4.8984743
		50	6.3201370	7.2600308
		75	9.6855618	11.2510938
		90	12.6722738	17.0697588
		95	16.9623822	19.4452167
Tukey's Hinges	Mahalanobis Distance	25	4.0499132	4.9117837
		50	6.3201370	7.2600308
		75	9.6747927	11.2510938

a. Unless otherwise noted, bootstrap results are based on 500 bootstrap samples

Extreme Values

		Case Number		Value
Mahalanobis Distance	Highest	1	1	23.79373
		2	2	23.68688
		3	3	23.49654
		4	4	23.04636
		5	5	22.74173
	Lowest	1	366	1.27656
		2	365	1.47344
		3	364	1.56851
		4	363	1.62831
		5	362	1.67551

Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Mahalanobis Distance	368	100.0%	0	0.0%	368	100.0%

Descriptives

		Statistic	Std. Error	
Mahalanobis Distance	Mean	8.3762542	.25396581	
	95% Confidence Interval for Mean	Lower Bound	7.8768434	
		Upper Bound	8.8756649	
		5% Trimmed Mean	7.9916427	
	Median	7.0804467		
	Variance	23.735		
	Std. Deviation	4.87190892		
	Minimum	.11320		
	Maximum	25.47917		
	Range	25.36597		
	Interquartile Range	6.16858		
	Skewness	1.190	.127	
	Kurtosis	1.231	.254	

M-Estimators

	Huber's M- Estimator ^a	Tukey's Biweight ^b	Hampel's M- Estimator ^c	Andrews' Wave ^d
Mahalanobis Distance	7.4775777	7.0977164	7.5443414	7.0914197

- a. The weighting constant is 1.339.
- b. The weighting constant is 4.685.
- c. The weighting constants are 1.700, 3.400, and 8.500
- d. The weighting constant is $1.340 \cdot \pi$.

Percentiles

		Percentiles			
		5	10	25	50
Weighted Average(Definition 1)	Mahalanobis Distance	2.7865149	3.6109737	4.7760401	7.0804467
Tukey's Hinges	Mahalanobis Distance			4.7889951	7.0804467

Percentiles

		Percentiles		
		75	90	95
Weighted Average(Definition 1)	Mahalanobis Distance	10.9446177	14.6915662	19.3121611
Tukey's Hinges	Mahalanobis Distance	10.9408341		

Extreme Values

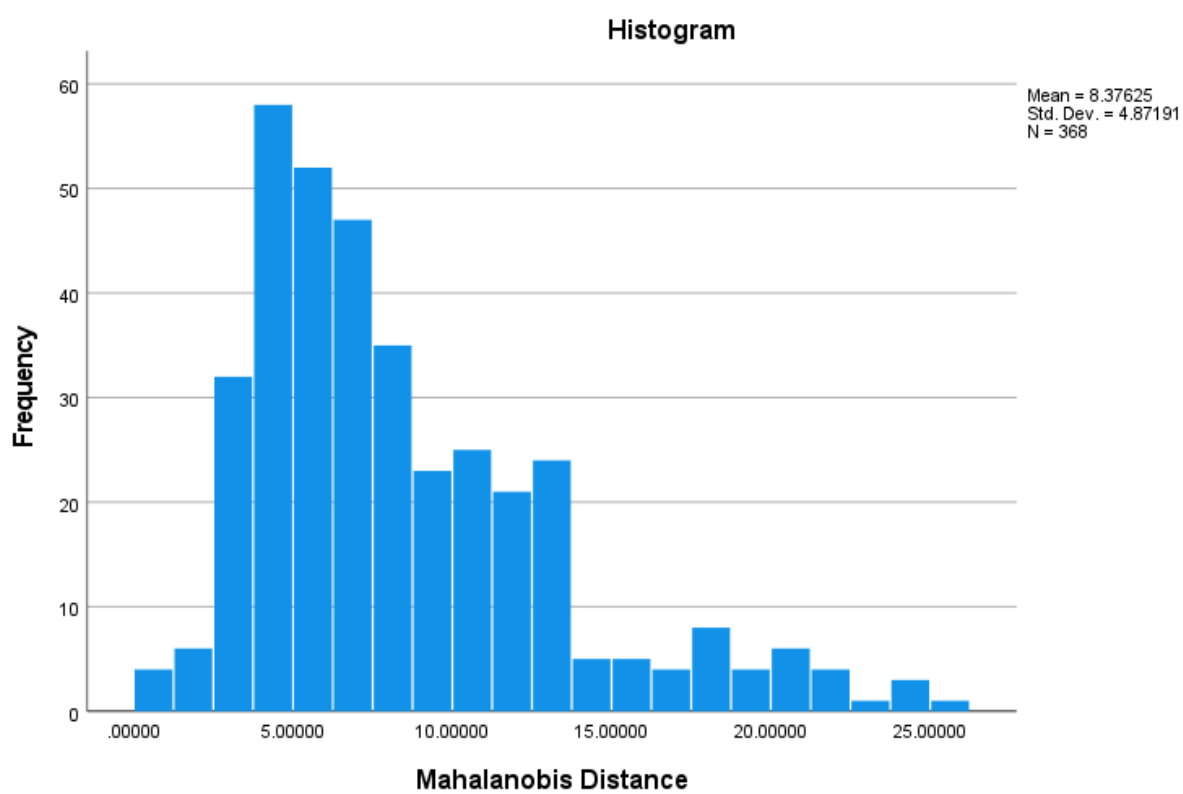
		Case Number		Value
Mahalanobis Distance	Highest	1	1	25.47917
		2	2	24.39951
		3	3	24.13595
		4	4	24.04491
		5	5	23.58781
	Lowest	1	368	.11320
		2	367	.11320
		3	366	.16990
		4	365	1.12682
		5	364	1.43447

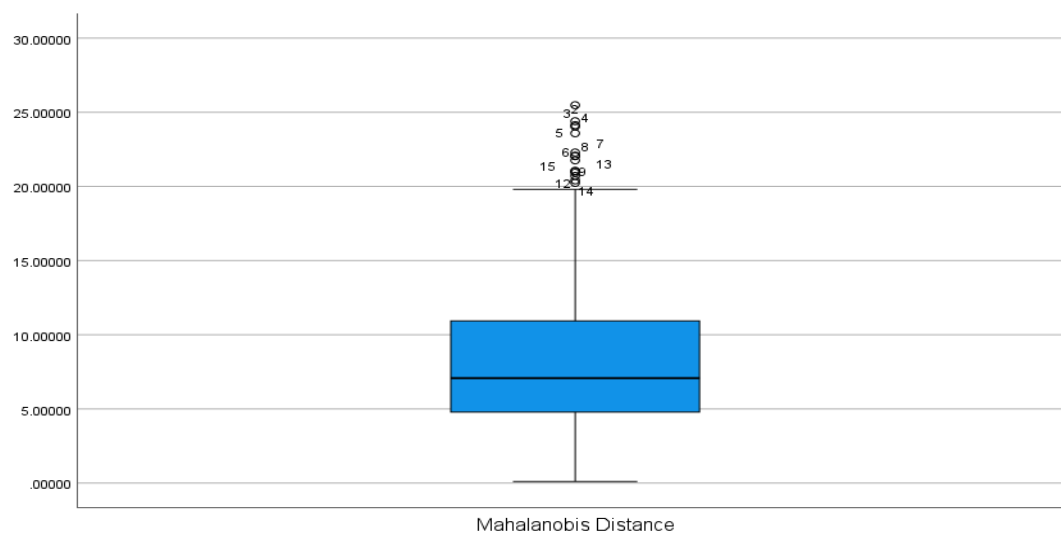
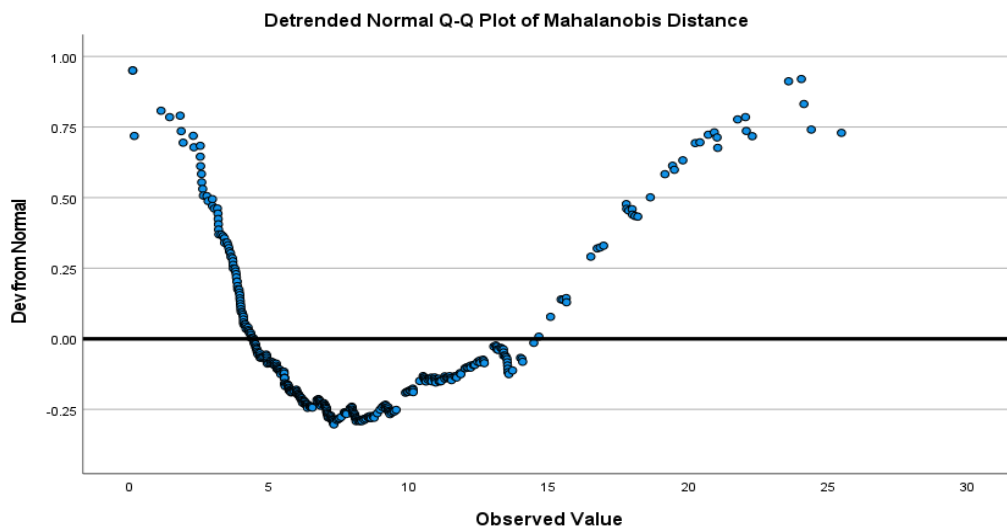
Tests of Normality

	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mahalanobis Distance	.122	368	.000	.906	368	.000

Mahalanobis Distance

a. Lilliefors Significance Correction





Appendix E:

Normality and Scatter Plot

Descriptive Statistics

	Mean	Std. Deviation	N
CSU	5.6739	1.44176	368
TSEV	4.7745	1.86735	368
TSUS	3.2140	1.51372	368
SEFF	4.8092	1.30504	368
RESP	4.5370	1.05863	368
PERF	4.6984	1.36721	368
SINF	4.9647	1.33751	368
ATT	4.0054	1.42297	368
PM	5.6241	1.34295	368

Correlations

		CSU	TSEV	TSUS	SEFF	RESP	PERF
Pearson Correlation	CSU	1.000	.447	-.075	.552	.737	.435
	TSEV	.447	1.000	.123	.289	.328	.191
	TSUS	-.075	.123	1.000	.045	.017	.166
	SEFF	.552	.289	.045	1.000	.619	.508
	RESP	.737	.328	.017	.619	1.000	.567
	PERF	.435	.191	.166	.508	.567	1.000
	SINF	.583	.331	.093	.499	.666	.521
	ATT	.123	-.093	.328	.405	.349	.546
	PM	.820	.434	-.110	.527	.710	.465
Sig. (1-tailed)	CSU	.	.000	.075	.000	.000	.000
	TSEV	.000	.	.009	.000	.000	.000
	TSUS	.075	.009	.	.193	.373	.001
	SEFF	.000	.000	.193	.	.000	.000
	RESP	.000	.000	.373	.000	.	.000
	PERF	.000	.000	.001	.000	.000	.
	SINF	.000	.000	.038	.000	.000	.000
	ATT	.009	.037	.000	.000	.000	.000
	PM	.000	.000	.018	.000	.000	.000
N	CSU	368	368	368	368	368	368

TSEV	368	368	368	368	368	368
TSUS	368	368	368	368	368	368
SEFF	368	368	368	368	368	368
RESP	368	368	368	368	368	368
PERF	368	368	368	368	368	368
SINF	368	368	368	368	368	368
ATT	368	368	368	368	368	368
PM	368	368	368	368	368	368

Correlations

		SINF	ATT	PM
Pearson Correlation	CSU	.583	.123	.820
	TSEV	.331	-.093	.434
	TSUS	.093	.328	-.110
	SEFF	.499	.405	.527
	RESP	.666	.349	.710
	PERF	.521	.546	.465
	SINF	1.000	.403	.601
	ATT	.403	1.000	.177
	PM	.601	.177	1.000
Sig. (1-tailed)	CSU	.000	.009	.000
	TSEV	.000	.037	.000
	TSUS	.038	.000	.018
	SEFF	.000	.000	.000
	RESP	.000	.000	.000
	PERF	.000	.000	.000
	SINF	.	.000	.000
	ATT	.000	.	.000
	PM	.000	.000	.
N	CSU	368	368	368
	TSEV	368	368	368
	TSUS	368	368	368
	SEFF	368	368	368
	RESP	368	368	368
	PERF	368	368	368
	SINF	368	368	368
	ATT	368	368	368
	PM	368	368	368

Variables Entered/Removed			
Model	Variables Entered	Variables Removed	Method
1	PM, TSUS, ATT, TSEV, SEFF, PERF, SINF, RESP ^b		. Enter

a. Dependent Variable: CSU

b. All requested variables entered.

Model Summary							
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics		
					R Square Change	F Change	df1
1	.862 ^a	.743	.737	.73902	.743	129.727	8

Model Summary			
Model	df2	Change Statistics	
		Sig. F Change	
1	359	.000	

a. Predictors: (Constant), PM, TSUS, ATT, TSEV, SEFF, PERF, SINF, RESP

b. Dependent Variable: CSU

ANOVA						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	566.802	8	70.850	129.727	.000 ^b
	Residual	196.067	359	.546		
	Total	762.870	367			

a. Dependent Variable: CSU

b. Predictors: (Constant), PM, TSUS, ATT, TSEV, SEFF, PERF, SINF, RESP

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.169	.208		.814	.416
	TSEV	.050	.025	.065	2.015	.045
	TSUS	.001	.029	.001	.040	.968
	SEFF	.115	.040	.104	2.845	.005
	RESP	.391	.062	.287	6.310	.000
	PERF	.009	.040	.009	.229	.819
	SINF	.059	.042	.055	1.390	.165
	ATT	-.134	.038	-.132	-3.563	.000
	PM	.557	.046	.519	12.164	.000

Model		95.0% Confidence Interval for B		Correlations			Collinearity Statistics
		Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance
1	(Constant)	-.240	.579				
	TSEV	.001	.100	.447	.106	.054	.681
	TSUS	-.055	.058	-.075	.002	.001	.789
	SEFF	.035	.194	.552	.148	.076	.535
	RESP	.269	.513	.737	.316	.169	.345
	PERF	-.069	.087	.435	.012	.006	.508
	SINF	-.024	.142	.583	.073	.037	.465
	ATT	-.208	-.060	.123	-.185	-.095	.518
	PM	.467	.647	.820	.540	.325	.393

Collinearity Statistics

Model	VIF	
1	(Constant)	
	TSEV	1.468
	TSUS	1.267
	SEFF	1.869
	RESP	2.898
	PERF	1.967
	SINF	2.148
	ATT	1.930
	PM	2.544

a. Dependent Variable: CSU

Model		Coefficient Correlations ^a						
		PM	TSUS	ATT	TSEV	SEFF		
1	Correlations	PM	1.000	.220	.089	-.255	-.109	
		TSUS	.220	1.000	-.322	-.276	.069	
		ATT	.089	-.322	1.000	.339	-.226	
		TSEV	-.255	-.276	.339	1.000	-.143	
		SEFF	-.109	.069	-.226	-.143	1.000	
		PERF	-.117	-.053	-.363	-.038	-.109	
		SINF	-.213	-.024	-.211	-.141	-.009	
		RESP	-.402	.003	-.016	.013	-.271	
	Covariances	PM	.002	.000	.000	.000	.000	
		TSUS	.000	.001	.000	.000	7.961E-5	
		ATT	.000	.000	.001	.000	.000	
		TSEV	.000	.000	.000	.001	.000	
		SEFF	.000	7.961E-5	.000	.000	.002	
		PERF	.000	-5.989E-5	-.001	-3.746E-5	.000	
	SINF	.000	-2.965E-5	.000	.000	-1.537E-5		
	RESP	-.001	5.605E-6	-3.695E-5	1.967E-5	-.001		

Model		Coefficient Correlations ^a				
		PERF	SINF	RESP		
1	Correlations	PM	-.117	-.213	-.402	
		TSUS	-.053	-.024	.003	
		ATT	-.363	-.211	-.016	
		TSEV	-.038	-.141	.013	
		SEFF	-.109	-.009	-.271	
		PERF	1.000	-.083	-.175	
		SINF	-.083	1.000	-.295	
		RESP	-.175	-.295	1.000	
	Covariances	PM	.000	.000	-.001	
		TSUS	-5.989E-5	-2.965E-5	5.605E-6	
		ATT	-.001	.000	-3.695E-5	
		TSEV	-3.746E-5	.000	1.967E-5	
		SEFF	.000	-1.537E-5	-.001	
		PERF	.002	.000	.000	
	SINF	.000	.002	-.001		
	RESP	.000	-.001	.004		

a. Dependent Variable: CSU

Collinearity Diagnostics^a

Model	Dimension	Eigenvalue	Condition	Variance Proportions			
			Index	(Constant)	TSEV	TSUS	SEFF
1	1	8.501	1.000	.00	.00	.00	.00
	2	.186	6.762	.00	.03	.55	.00
	3	.135	7.924	.00	.36	.11	.00
	4	.046	13.580	.13	.53	.10	.00
	5	.035	15.541	.08	.01	.02	.42
	6	.033	15.976	.03	.02	.05	.18
	7	.031	16.579	.50	.02	.11	.25
	8	.019	21.063	.25	.00	.05	.09
	9	.013	25.243	.00	.03	.02	.05

Collinearity Diagnostics^a

Model	Dimension	Variance Proportions				
		RESP	PERF	SINF	ATT	PM
1	1	.00	.00	.00	.00	.00
	2	.00	.00	.00	.02	.01
	3	.00	.02	.00	.12	.00
	4	.02	.06	.01	.37	.04
	5	.00	.26	.19	.08	.01
	6	.00	.50	.19	.28	.00
	7	.01	.10	.19	.02	.00
	8	.11	.06	.38	.11	.43
	9	.84	.01	.04	.00	.52

a. Dependent Variable: CSU

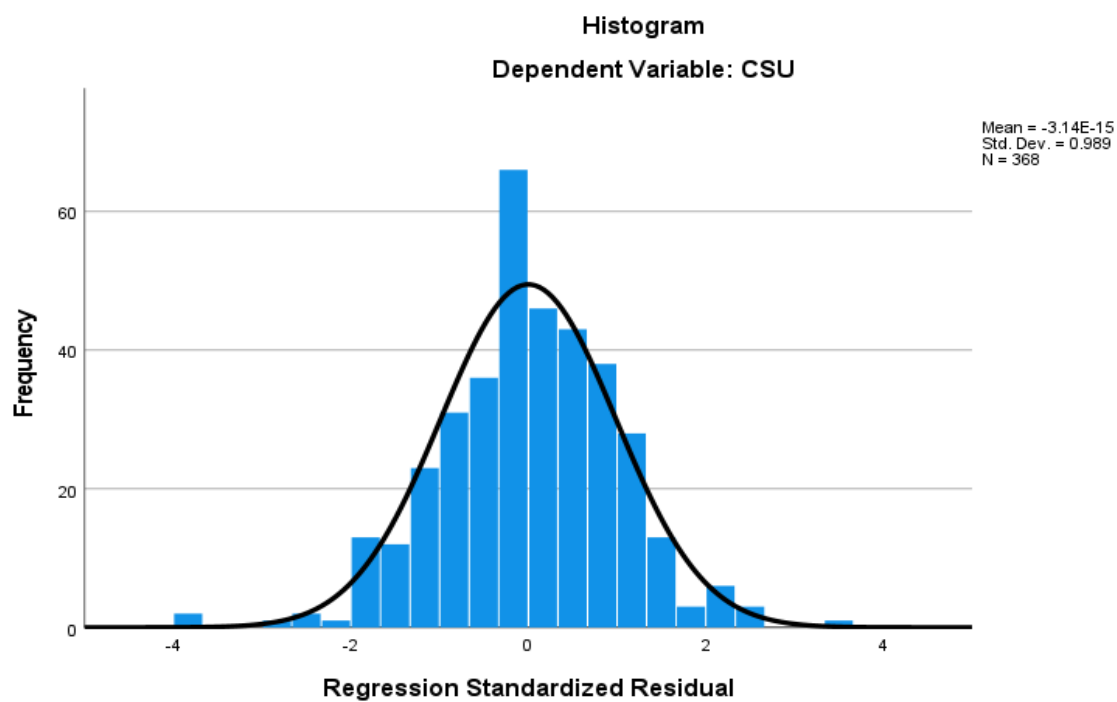
Residuals Statistics^a

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.1694	7.6355	5.6739	1.24275	368
Std. Predicted Value	-3.625	1.578	.000	1.000	368
Standard Error of Predicted Value	.058	.198	.112	.030	368
Adjusted Predicted Value	1.1784	7.6706	5.6736	1.24345	368
Residual	-2.84355	2.67932	.00000	.73092	368

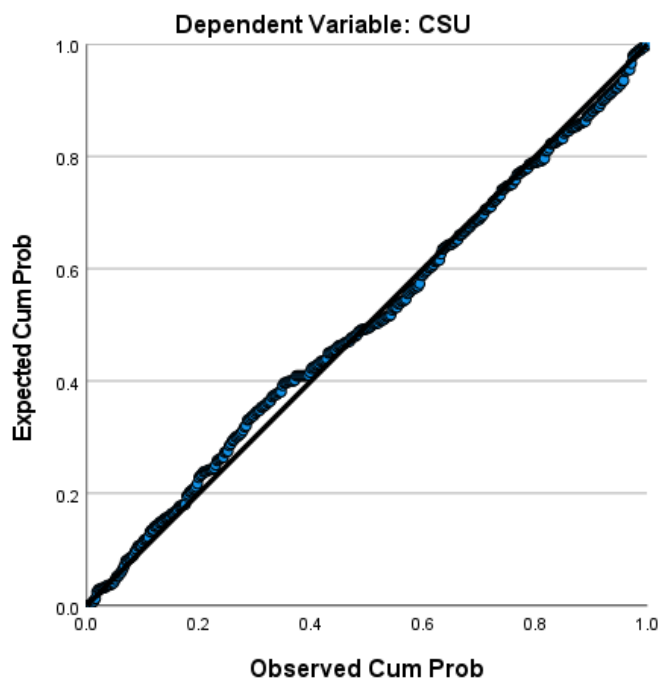
Std. Residual	-3.848	3.626	.000	.989	368
Stud. Residual	-3.894	3.660	.000	1.003	368
Deleted Residual	-2.91247	2.73054	.00028	.75115	368
Stud. Deleted Residual	-3.973	3.725	.000	1.007	368
Mahal. Distance	1.277	25.230	7.978	4.836	368
Cook's Distance	.000	.055	.003	.006	368
Centered Leverage Value	.003	.069	.022	.013	368

a. Dependent Variable: CSU

Charts

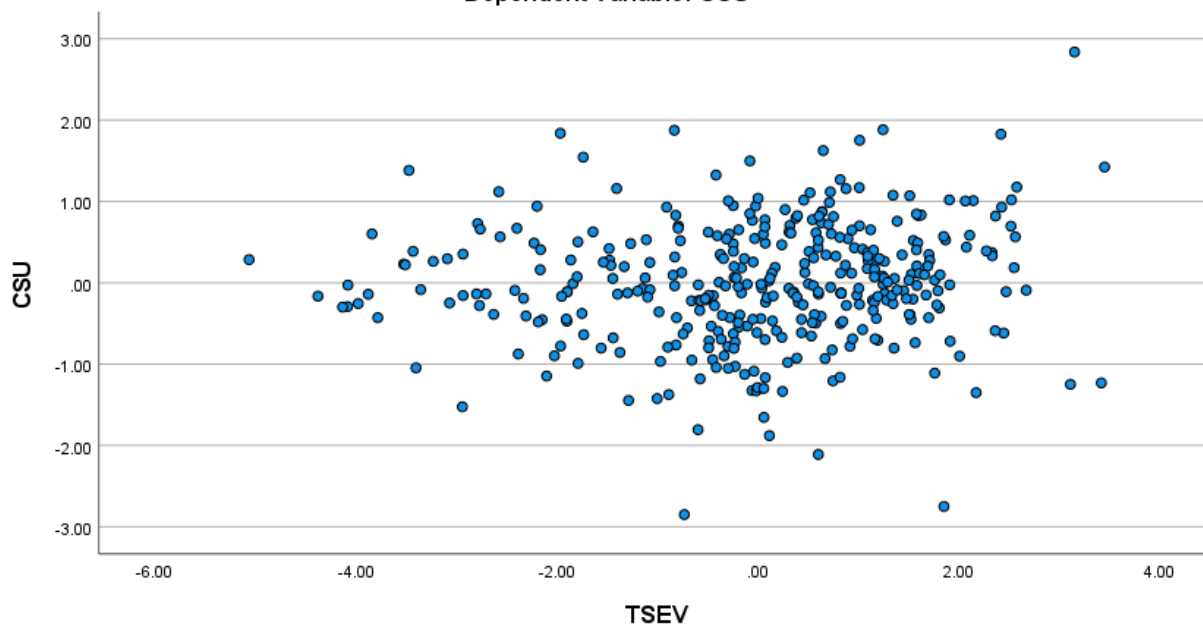


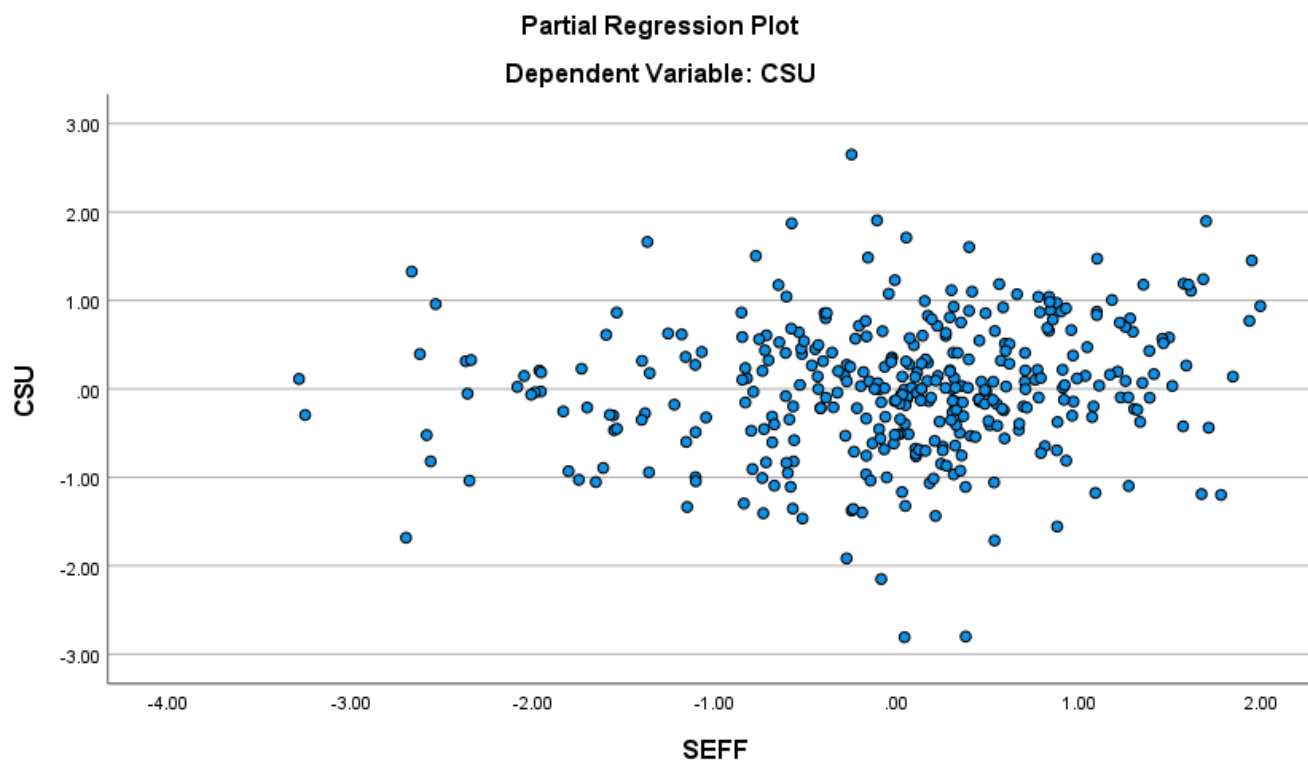
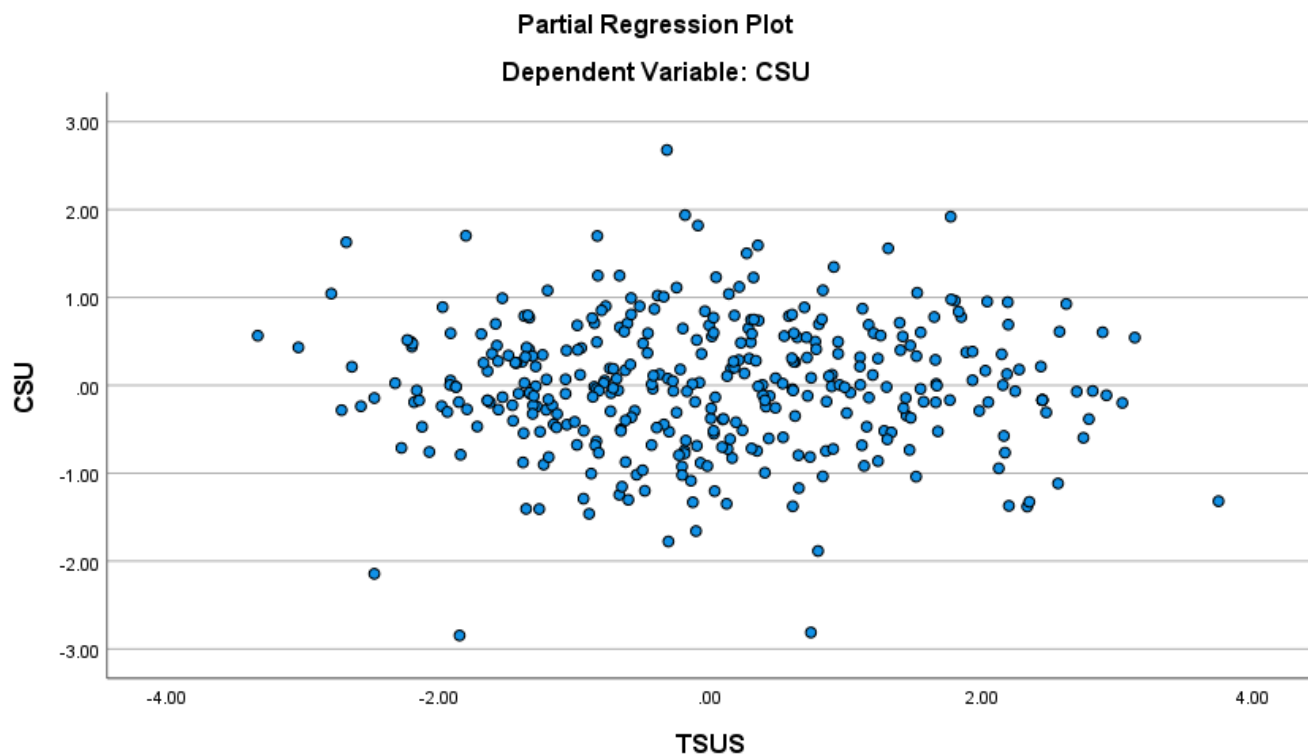
Normal P-P Plot of Regression Standardized Residual

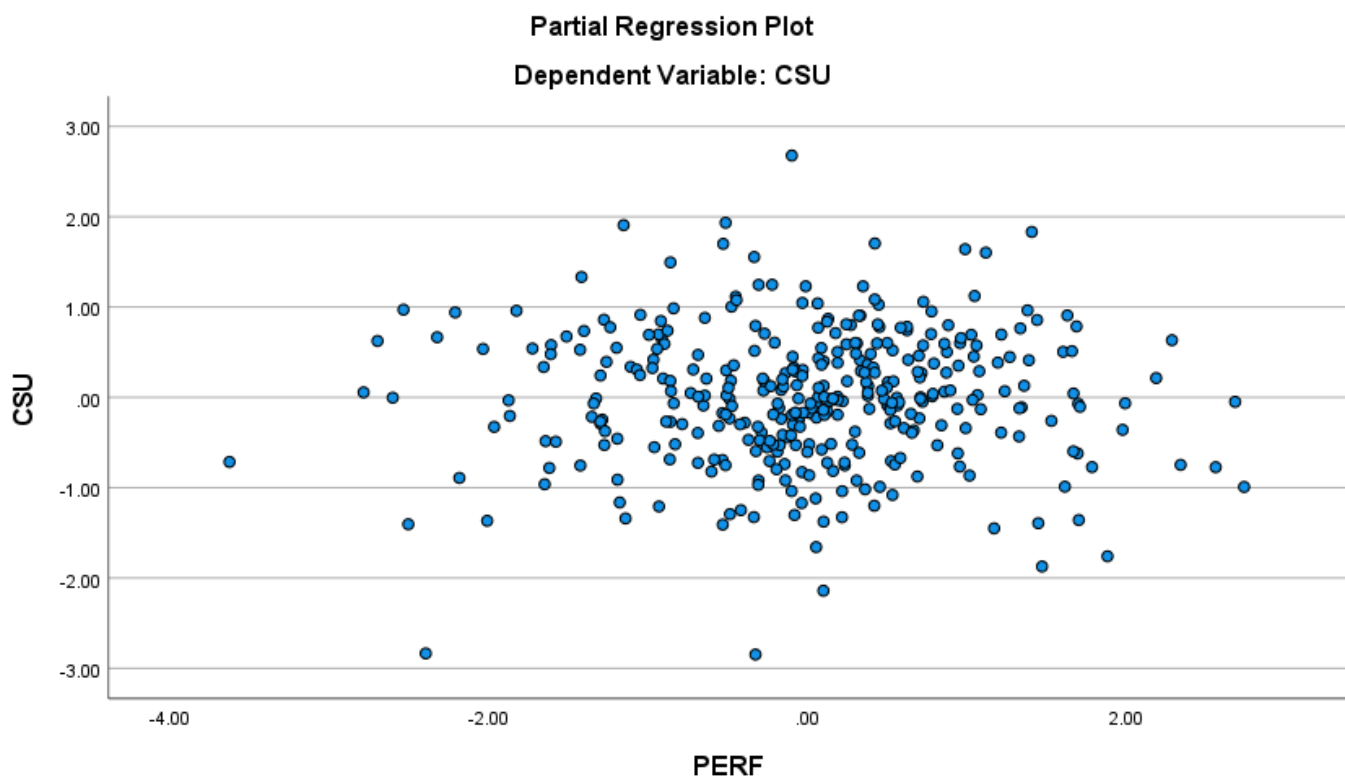
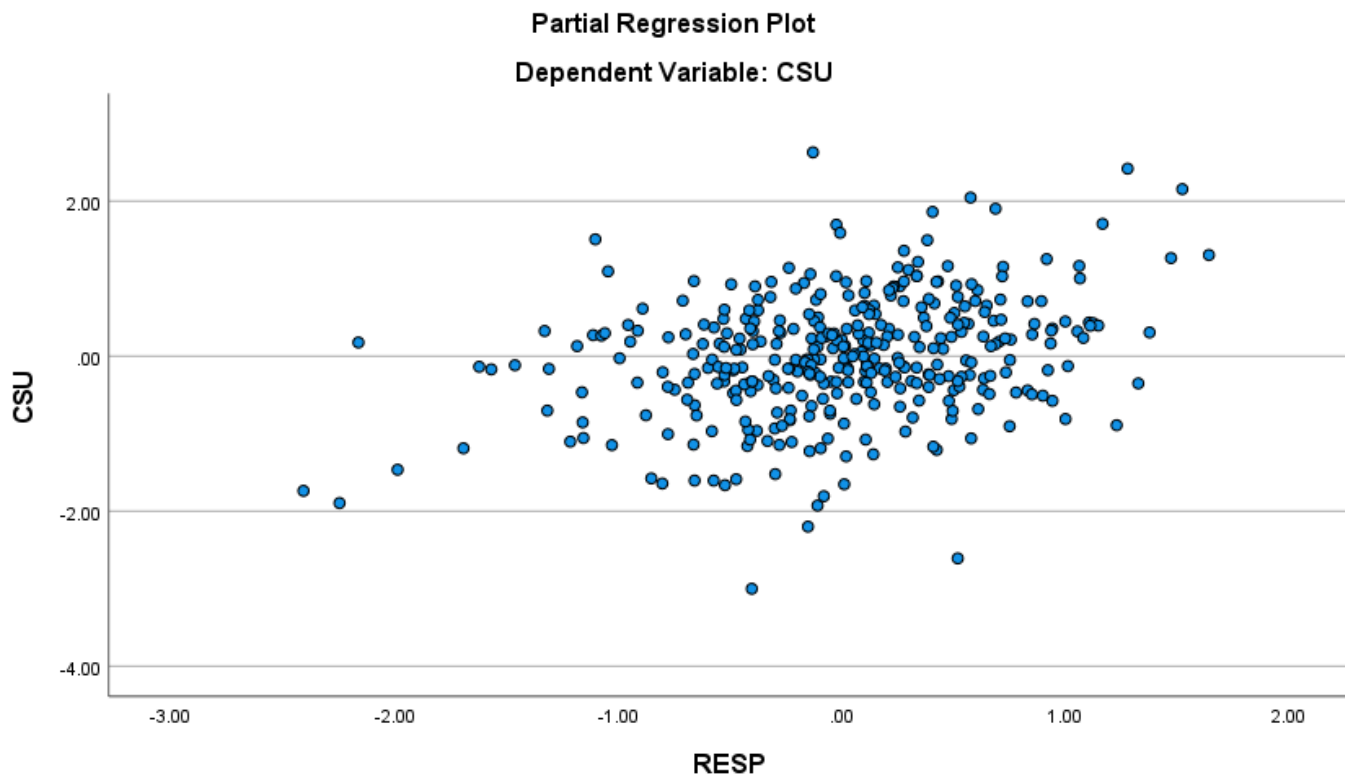


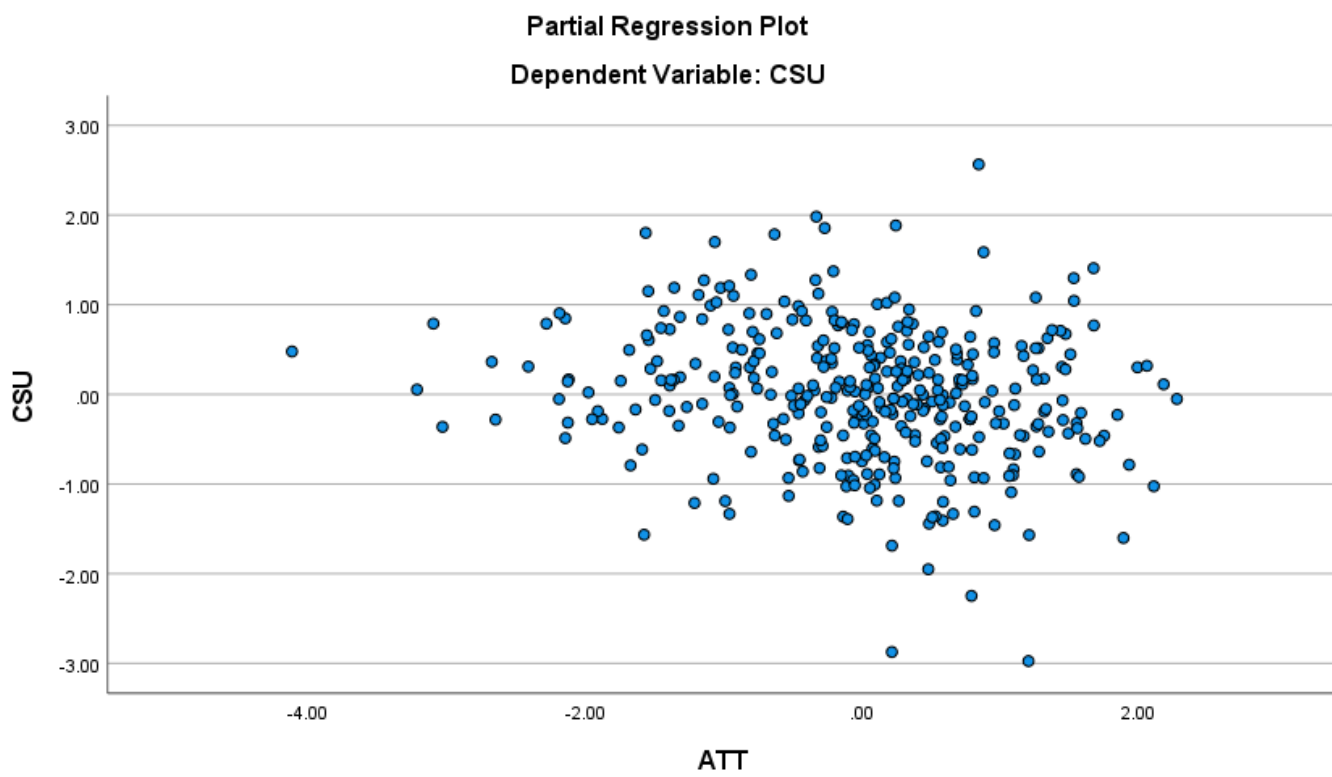
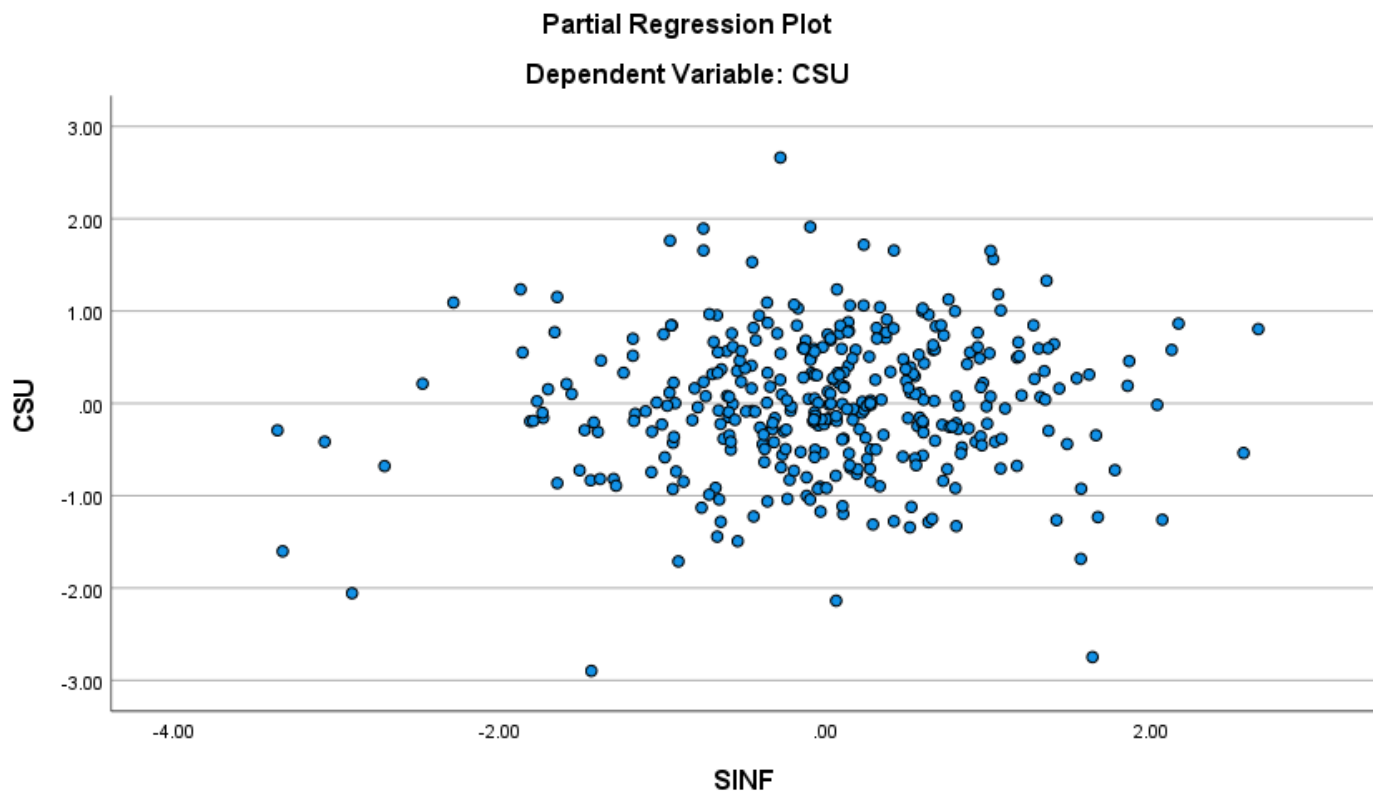
Partial Regression Plot

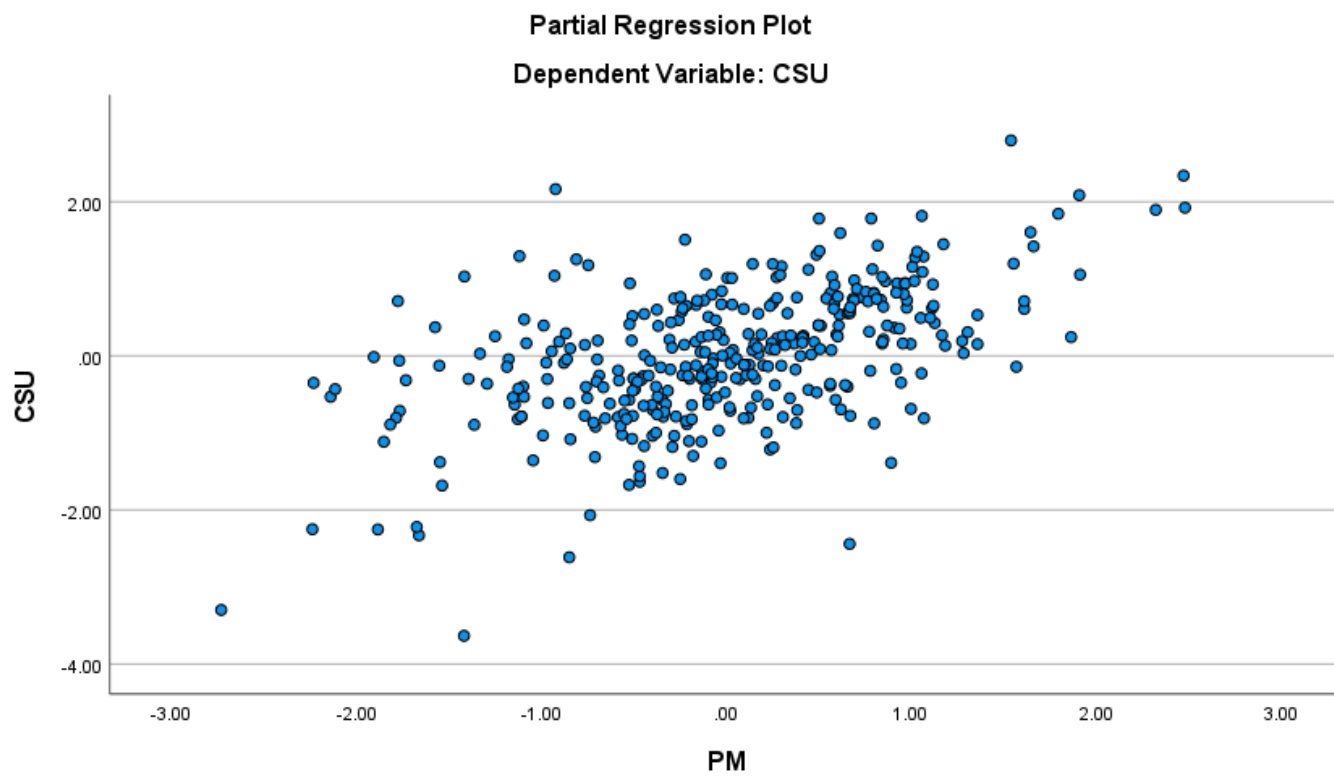
Dependent Variable: CSU





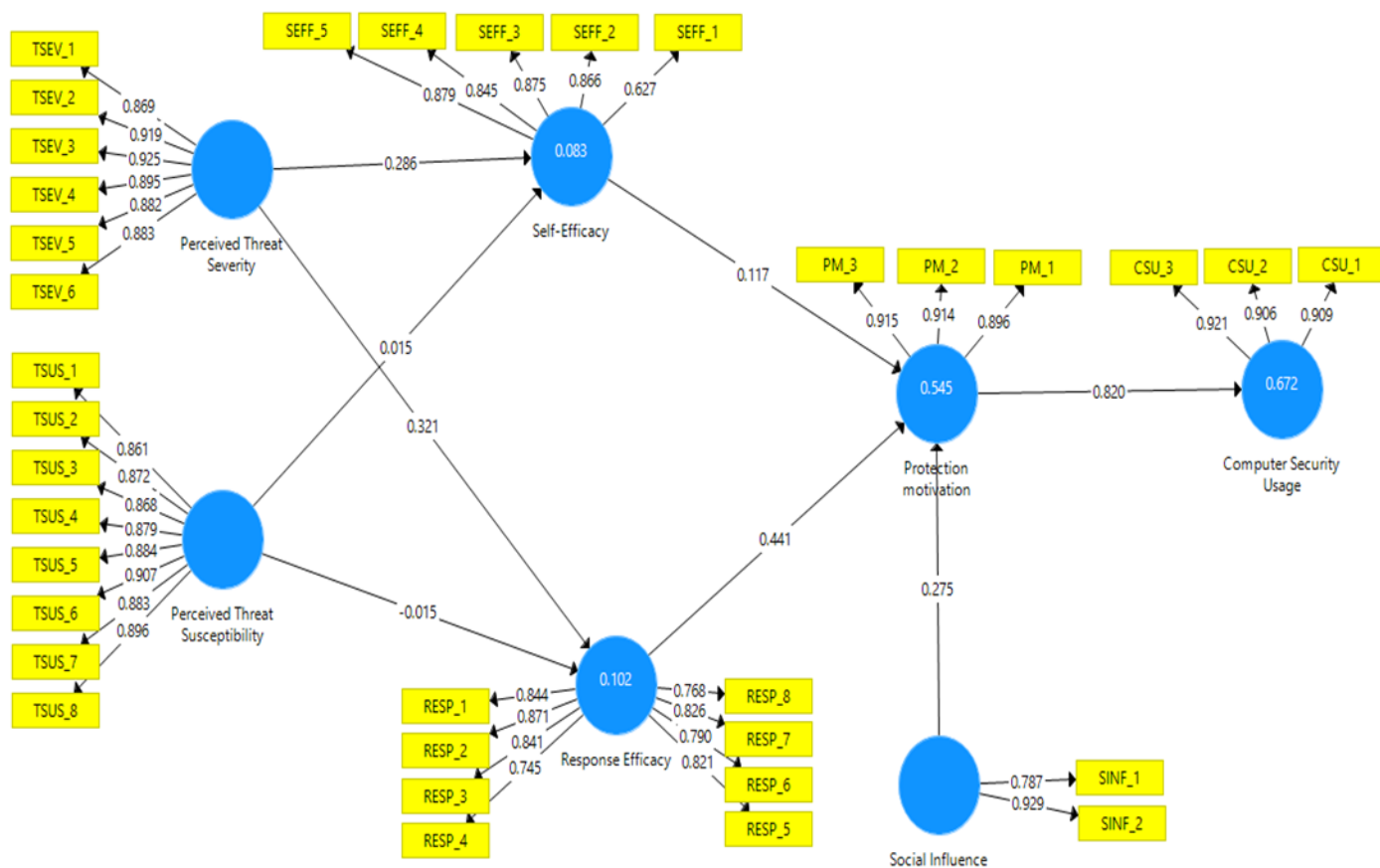






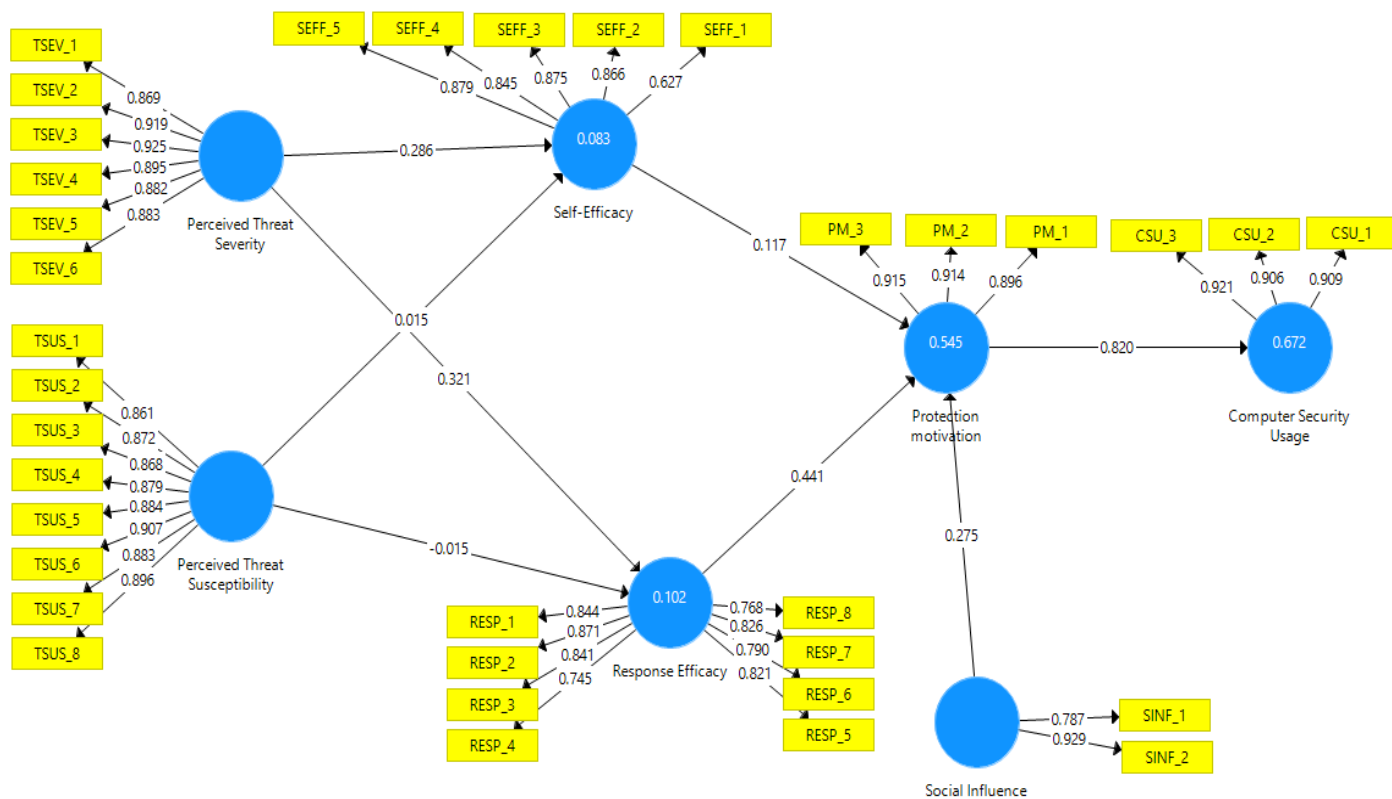
Appendix F:

PLS Analysis with Factor Loadings



Appendix G:

PLS Analysis after deleting outlier



Appendix H:

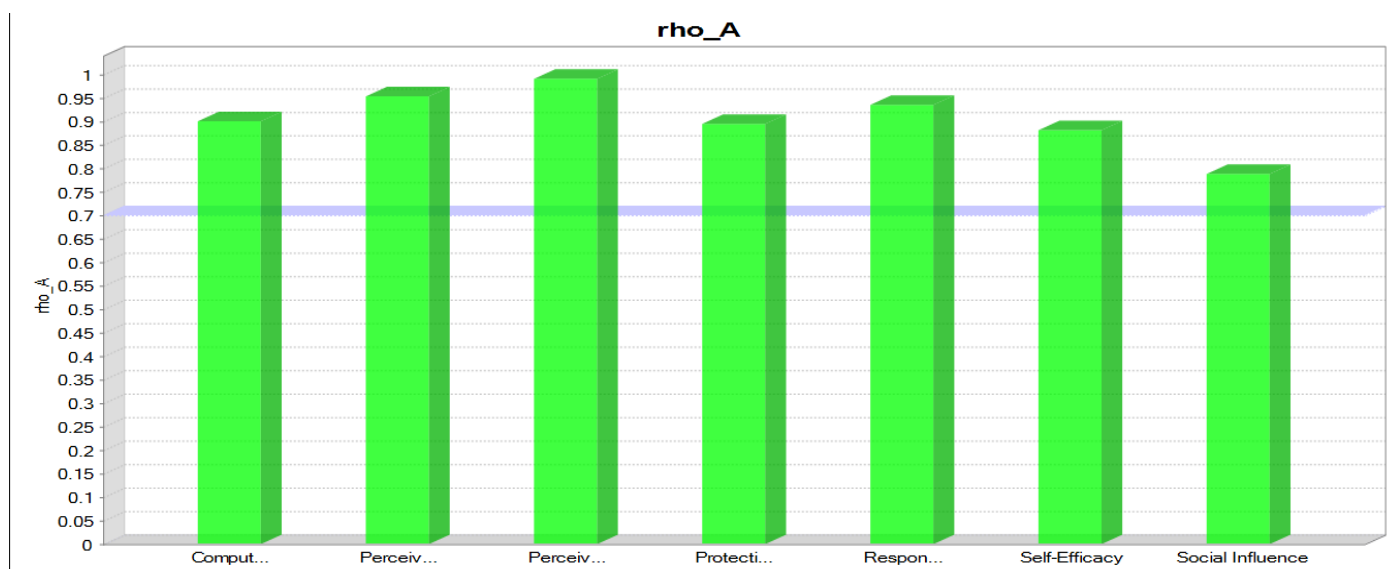
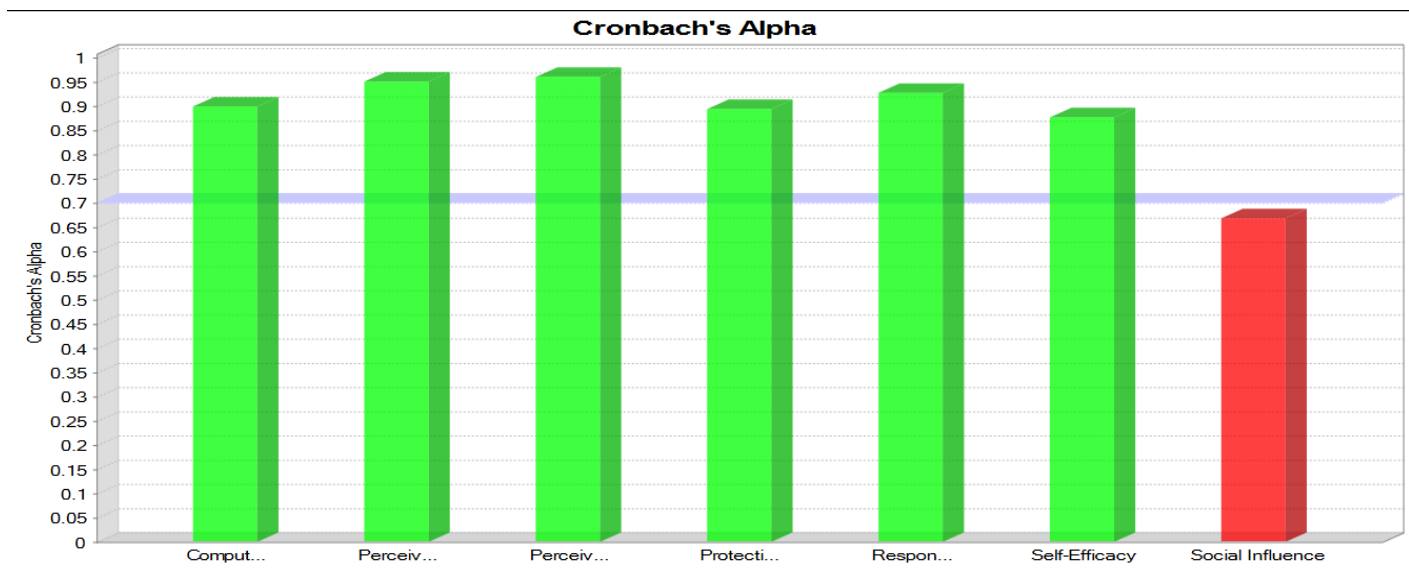
Model fit, Reliability, Validity, Coefficient and Outer Loading

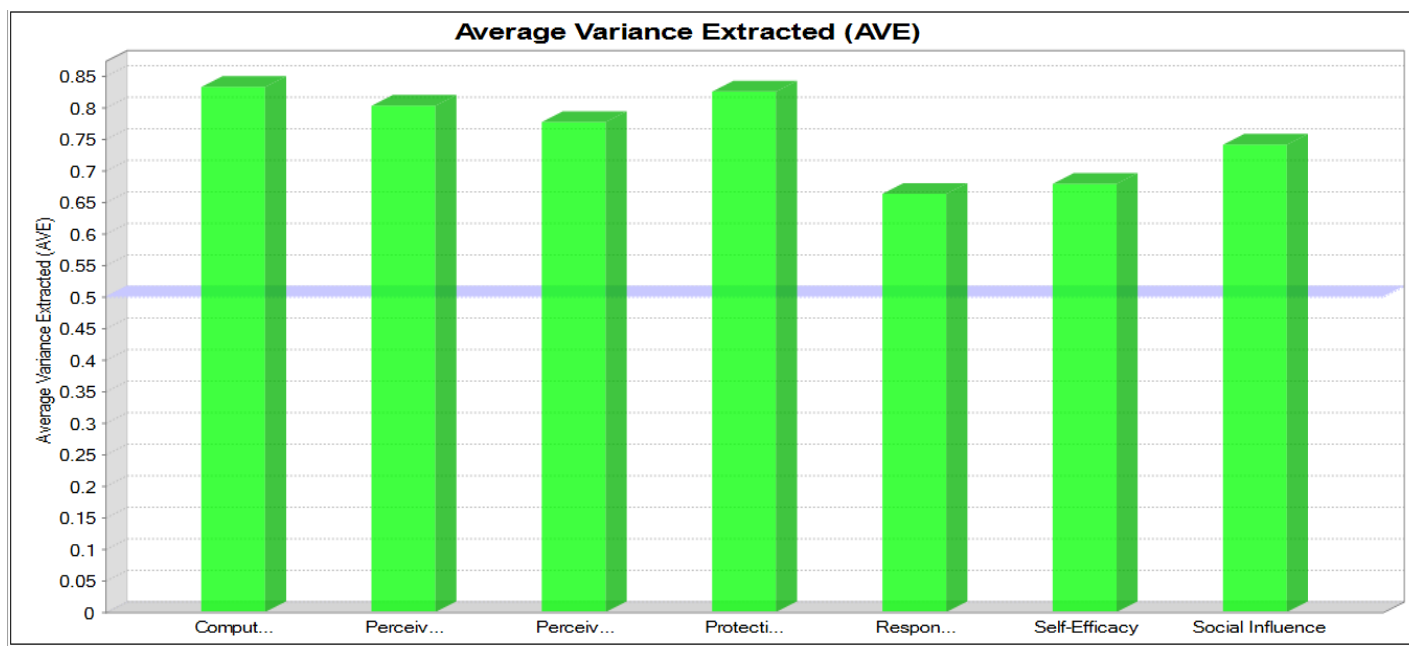
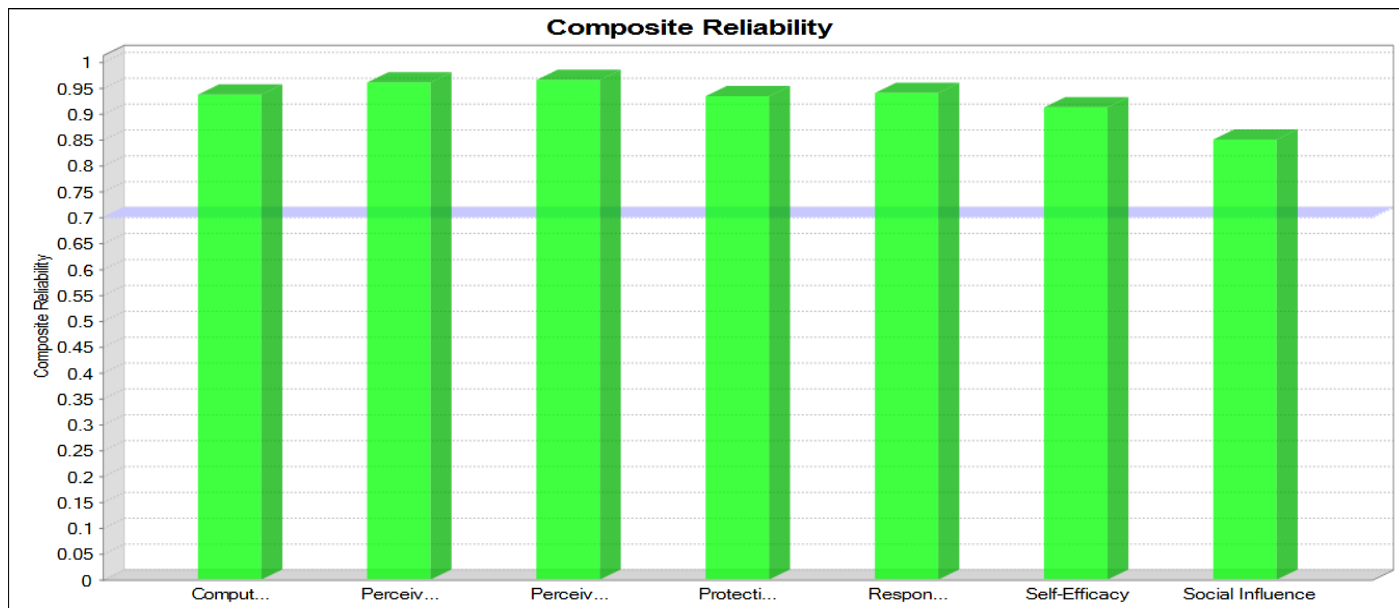
Model_Fit

Fit Summary		rms Theta	
	Saturated Model	Estimated Model	
SRMR	0.057	0.163	
d_ULS	2.013	16.640	
d_G	0.877	1.193	
Chi-Square	1828.854	2189.066	
NFI	0.849	0.819	

Construct Reliability and Validity

Matrix	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Computer Security Usage	0.899	0.900	0.937	0.832
Perceived Threat Severity	0.951	0.953	0.961	0.802
Perceived Threat Susceptibility	0.960	0.991	0.965	0.777
Protection motivation	0.894	0.895	0.934	0.825
Response Efficacy	0.928	0.935	0.940	0.663
Self-Efficacy	0.877	0.881	0.912	0.679
Social Influence	0.668	0.788	0.850	0.741





Discriminant Validity

Fornell-Larcker Criterion		Cross Loadings		Heterotrait-Monotrait Ratio (HTMT)		Heterotrait-Monotrait Ratio (HTMT)		Copy	
	Computer Security Usage	Perceived Threat Severity	Perceived Threat Susceptibility	Protection motivation	Response Efficacy	Self-Efficacy	Social Influence		
Computer Security Usage	0.912								
Perceived Threat Severity	0.448	0.896							
Perceived Threat Susceptibility	-0.075	0.120	0.881						
Protection motivation	0.820	0.435	-0.105	0.908					
Response Efficacy	0.730	0.319	0.023	0.700	0.814				
Self-Efficacy	0.554	0.288	0.049	0.528	0.618	0.824			
Social Influence	0.611	0.350	0.079	0.635	0.682	0.506	0.861		

Item-to-construct correlations

Correlations												
		I find the use of anti-spyware software useful in my job.	Using anti-spyware software enables me to accomplish tasks more quickly.	PERF	People who influence my behavior think that I should use anti-spyware software.	In general, my organization has supported using and providing anti-spyware software.	SINF	Anti-spyware software makes work more interesting.	Working with anti-spyware software is fun.	I like working with anti-spyware software.	Working with anti-spyware software is enjoyable.	ATT
I find the use of anti-spyware software useful in my job.	Pearson Correlation	--										
	N	368										
Using anti-spyware software enables me to accomplish tasks more quickly.	Pearson Correlation	.560**	--									
	Sig. (2-tailed)	.000										
	N	368	368									
PERF	Pearson Correlation	.879**	.887**	--								
	Sig. (2-tailed)	.000	.000									
	N	368	368	368								
People who influence my behavior think that I should use anti-spyware software.	Pearson Correlation	.454**	.364**	.462**	--							
	Sig. (2-tailed)	.000	.000	.000								
	N	368	368	368	368							
In general, my organization has supported using and providing anti-spyware software.	Pearson Correlation	.495**	.286**	.441**	.502**	--						
	Sig. (2-tailed)	.000	.000	.000	.000							
	N	368	368	368	368	368						
SINF	Pearson Correlation	.547**	.376**	.521**	.872**	.861**	--					
	Sig. (2-tailed)	.000	.000	.000	.000	.000						
	N	368	368	368	368	368	368					
Anti-spyware software makes work more interesting.	Pearson Correlation	.365**	.563**	.527**	.425**	.263**	.399**	--				
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000					
	N	368	368	368	368	368	368	368				
Working with anti-spyware software is fun.	Pearson Correlation	.285**	.516**	.455**	.375**	.213**	.341**	.710**	--			
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000				
	N	368	368	368	368	368	368	368	368			
I like working with anti-spyware software.	Pearson Correlation	.357**	.471**	.469**	.339**	.317**	.378**	.616**	.729**	--		
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000			
	N	368	368	368	368	368	368	368	368	368		
Working with anti-spyware software is enjoyable.	Pearson Correlation	.328**	.495**	.467**	.316**	.202**	.300**	.639**	.737**	.727**	--	
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000		
	N	368	368	368	368	368	368	368	368	368	368	
ATT	Pearson Correlation	.380**	.583**	.546**	.414**	.282**	.403**	.844**	.906**	.874**	.885**	--
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	
	N	368	368	368	368	368	368	368	368	368	368	368

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

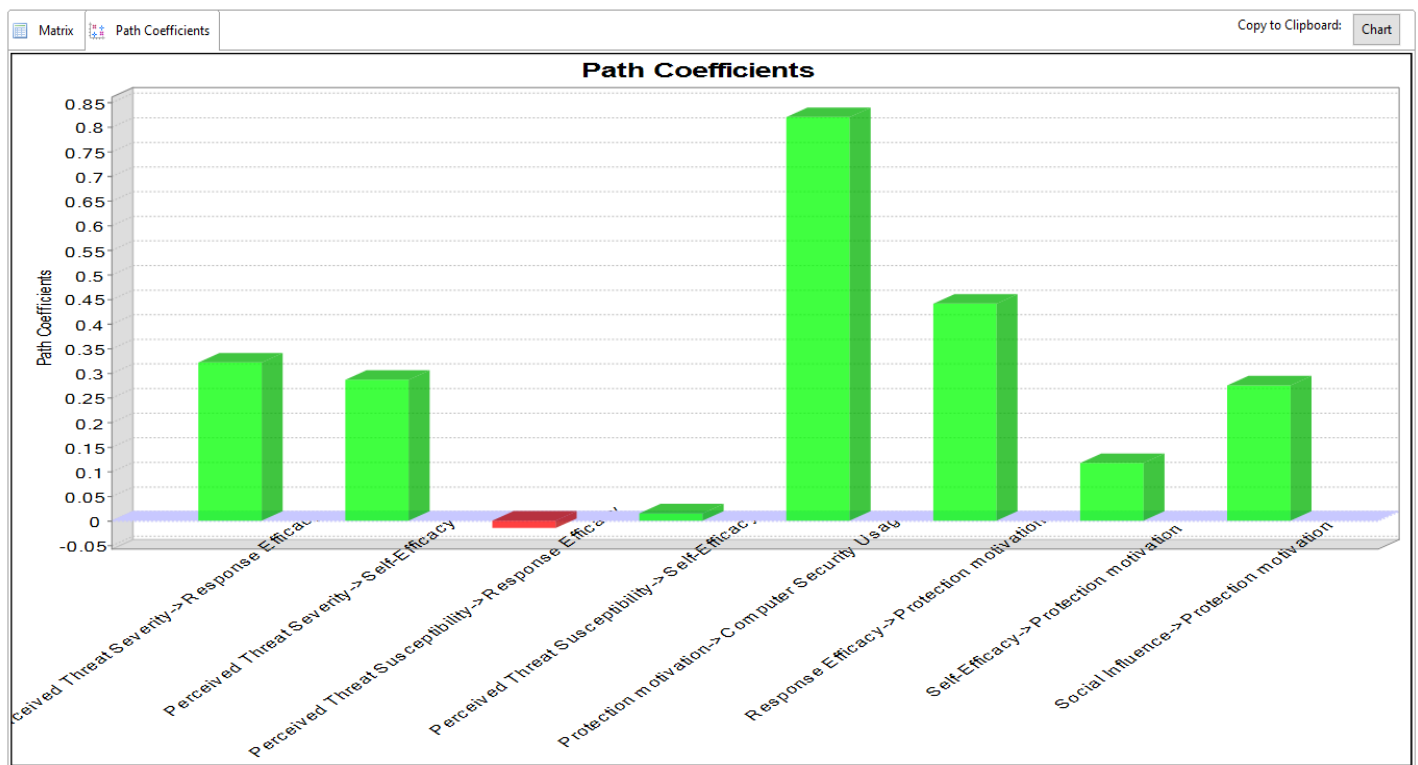
Outer Loadings

Matrix	Computer Security Usa...	Perceived Threat Severity	Perceived Threat Susceptibility	Protection motivation	Response Efficacy	Self-Efficacy	Social Influence
CSU_1	0.909						
CSU_2	0.906						
CSU_3	0.921						
PM_1				0.896			
PM_2				0.914			
PM_3				0.915			
RESP_1					0.844		
RESP_2					0.871		
RESP_3					0.841		
RESP_4					0.745		
RESP_5					0.821		
RESP_6					0.790		
RESP_7					0.826		
RESP_8					0.768		
SEFF_1						0.627	
SEFF_2						0.866	
SEFF_3						0.875	
SEFF_4						0.845	
SEFF_5						0.879	
SINF_1							0.787
SINF_2							0.929
TSEV_1		0.869					
TSEV_2		0.919					
TSEV_3		0.925					
TSEV_4		0.895					
TSEV_5		0.882					
TSEV_6		0.883					
TSUS_1			0.861				
TSUS_2			0.872				
TSUS_3			0.868				
TSUS_4			0.879				
TSUS_5			0.884				
TSUS_6			0.887				

Path Coefficients

	Computer Security Usage	Perceived Threat Severity	Perceived Threat Susceptibility	Protection motivation	Response Efficacy	Self-Efficacy	Social Influence
Computer Security Usage							
Perceived Threat Severity					0.321	0.286	
Perceived Threat Susceptibility					-0.015	0.015	
Protection motivation	0.820						
Response Efficacy				0.441			
Self-Efficacy				0.117			
Social Influence				0.275			

Path Coefficients



R Square

Matrix	R Square	R Square Adjusted
	R Square	R Square Adjusted
Computer Security Usage	0.672	0.671
Protection motivation	0.545	0.541
Response Efficacy	0.102	0.097
Self-Efficacy	0.083	0.078

Path Coefficients

Mean, STDEV, T-Values, P-Values	Confidence Intervals	Confidence Intervals Bias Corrected	Samples		
	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O /STDEV)	P Values
Perceived Threat Severity -> Response Efficacy	0.321	0.324	0.056	5.734	0.000
Perceived Threat Severity -> Self-Efficacy	0.286	0.289	0.058	4.906	0.000
Perceived Threat Susceptibility -> Response Efficacy	-0.015	-0.012	0.071	0.211	0.833
Perceived Threat Susceptibility -> Self-Efficacy	0.015	0.016	0.073	0.203	0.839
Protection motivation -> Computer Security Usage	0.820	0.821	0.020	41.423	0.000
Response Efficacy -> Protection motivation	0.441	0.444	0.062	7.150	0.000
Self-Efficacy -> Protection motivation	0.117	0.115	0.045	2.594	0.010
Social Influence -> Protection motivation	0.275	0.274	0.058	4.740	0.000

Composite Reliability

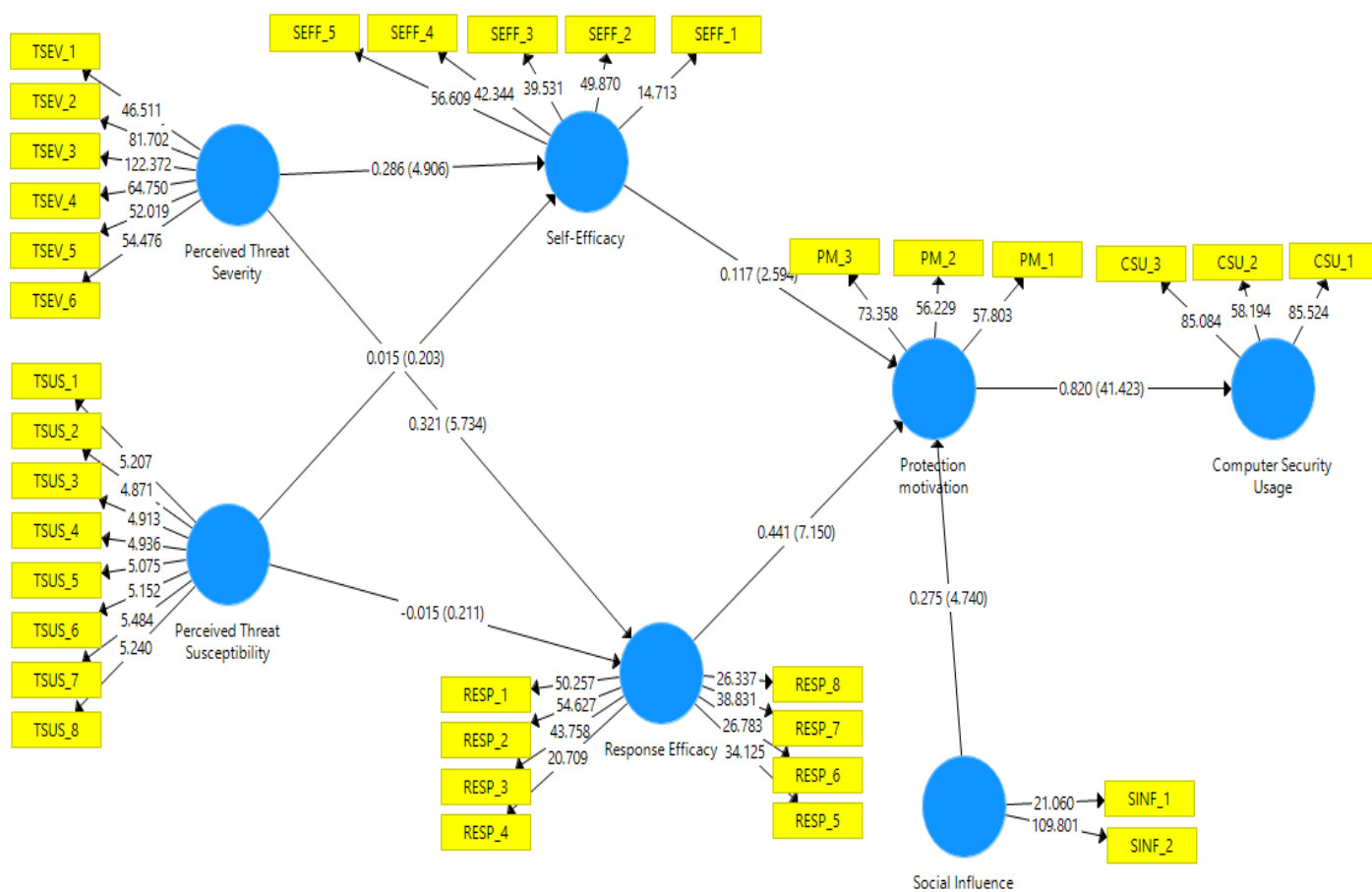
Mean, STDEV, T-Values, P-Values	Confidence Intervals	Confidence Intervals Bias Corrected	Samples		
	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O /STDEV)	P Values
Computer Security Usage	0.937	0.937	0.007	130.573	0.000
Perceived Threat Severity	0.961	0.960	0.004	234.073	0.000
Perceived Threat Susceptibility	0.965	0.946	0.090	10.771	0.000
Protection motivation	0.934	0.934	0.009	102.752	0.000
Response Efficacy	0.940	0.940	0.007	144.447	0.000
Self-Efficacy	0.912	0.912	0.008	116.765	0.000
Social Influence	0.850	0.848	0.018	47.364	0.000

Path Coefficients

Mean, STDEV, T-Values, P-Values	Confidence Intervals	Confidence Intervals Bias Corrected	Samples		
	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O /STDEV)	P Values
Perceived Threat Severity -> Response Efficacy	0.321	0.324	0.056	5.734	0.000
Perceived Threat Severity -> Self-Efficacy	0.286	0.289	0.058	4.906	0.000
Perceived Threat Susceptibility -> Response Efficacy	-0.015	-0.012	0.071	0.211	0.833
Perceived Threat Susceptibility -> Self-Efficacy	0.015	0.016	0.073	0.203	0.839
Protection motivation -> Computer Security Usage	0.820	0.821	0.020	41.423	0.000
Response Efficacy -> Protection motivation	0.441	0.444	0.062	7.150	0.000
Self-Efficacy -> Protection motivation	0.117	0.115	0.045	2.594	0.010
Social Influence -> Protection motivation	0.275	0.274	0.058	4.740	0.000

Total Effects

Mean, STDEV, T-Values, P-Values	Confidence Intervals	Confidence Intervals Bias Corrected	Samples		
	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O /STDEV)	P Values
Perceived Threat Severity -> Protection motivation	0.175	0.178	0.037	4.692	0.000
Perceived Threat Severity -> Response Efficacy	0.321	0.324	0.056	5.734	0.000
Perceived Threat Severity -> Self-Efficacy	0.286	0.289	0.058	4.906	0.000
Perceived Threat Susceptibility -> Computer Security Usage	-0.004	-0.003	0.031	0.129	0.898
Perceived Threat Susceptibility -> Protection motivation	-0.005	-0.004	0.038	0.129	0.897
Perceived Threat Susceptibility -> Response Efficacy	-0.015	-0.012	0.071	0.211	0.833
Perceived Threat Susceptibility -> Self-Efficacy	0.015	0.016	0.073	0.203	0.839
Protection motivation -> Computer Security Usage	0.820	0.821	0.020	41.423	0.000
Response Efficacy -> Computer Security Usage	0.361	0.364	0.053	6.828	0.000
Response Efficacy -> Protection motivation	0.441	0.444	0.062	7.150	0.000
Self-Efficacy -> Computer Security Usage	0.096	0.095	0.037	2.579	0.010
Self-Efficacy -> Protection motivation	0.117	0.115	0.045	2.594	0.010
Social Influence -> Computer Security Usage	0.225	0.225	0.048	4.704	0.000
Social Influence -> Protection motivation	0.275	0.274	0.058	4.740	0.000



Appendix I:

Descriptive variables

/STATISTICS=MEAN STDDEV MIN MAX KURTOSIS SKEWNESS.

Descriptives**Notes**

Output Created		26-NOV-2020 20:36:59
Comments		
Input	Data	C:\Users\tfofu\Dropbox\ _NSU__ISEC- 0885_Doctoral_Research\working\data\Computer Security Behaviors_2.sav
	Active Dataset	DataSet1
	File Label	File created by user 'asyncjobs_user' at Fri Oct 30 00:48:43 202
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	368
Missing Value Handling	Definition of Missing	User defined missing values are treated as missing.
	Cases Used	All non-missing data are used.

Syntax		DESCRIPTIVES VARIABLES=PERF /STATISTICS=MEAN STDDEV MIN MAX KURTOSIS SKEWNESS.
Resources	Processor Time	00:00:00.02
	Elapsed Time	00:00:00.01

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness	
						Statistic	Std. Error
PERF	368	1.00	7.00	4.6984	1.36721	-.346	.127
Valid N (listwise)	368						

Descriptive Statistics

	Statistic	Std. Error
		Kurtosis
PERF	-.090	.254
Valid N (listwise)		

FREQUENCIES VARIABLES=PERF

/STATISTICS=SKEWNESS SESKEW KURTOSIS SEKURT

/BARCHART FREQ

/ORDER=ANALYSIS.

Frequencies

Notes

Output Created		26-NOV-2020 20:39:07
Comments		
Input	Data	C:\Users\tfofu\Dropbox\ _NSU__ISEC- 0885_Doctoral_Research\working\data\Computer Security Behaviors_2.sav
	Active Dataset	DataSet1
	File Label	File created by user 'asyncjobs_user' at Fri Oct 30 00:48:43 202
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	368
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data.

Syntax		FREQUENCIES VARIABLES=PERF /STATISTICS=SKEWNESS SESKEW KURTOSIS SEKURT /BARCHART FREQ /ORDER=ANALYSIS.
Resources	Processor Time	00:00:00.44
	Elapsed Time	00:00:00.25

Statistics

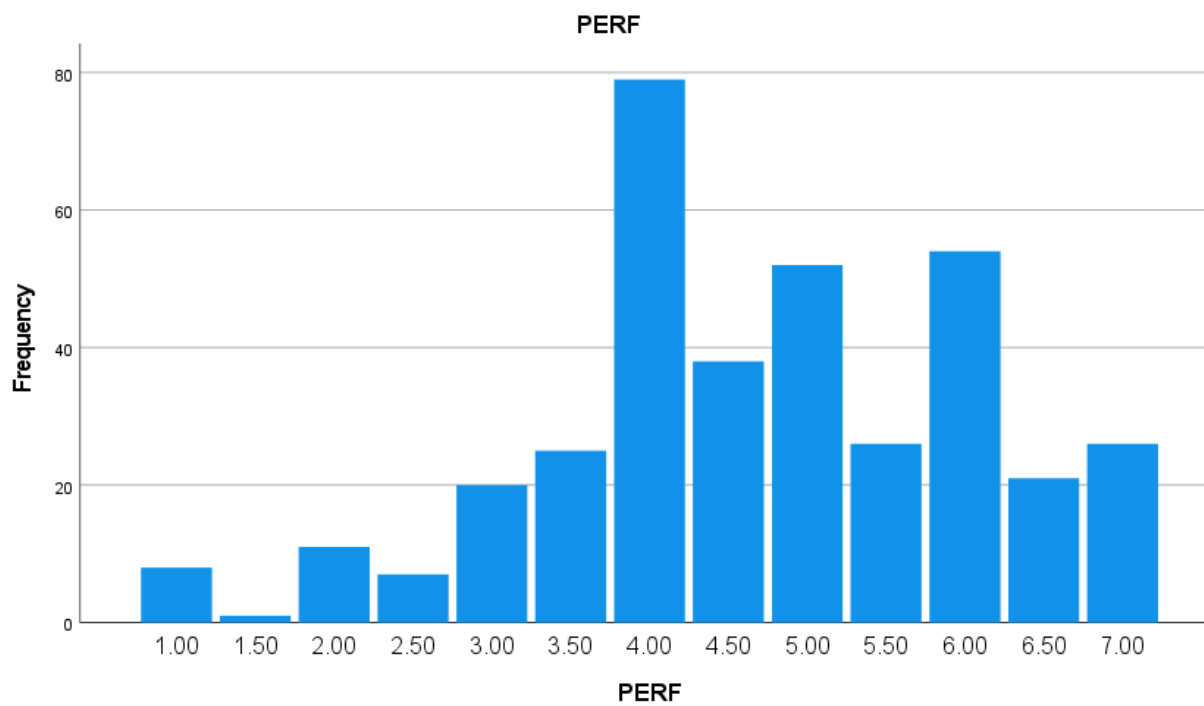
PERF

N	Valid	368
	Missing	0
Skewness		-.346
Std. Error of Skewness		.127
Kurtosis		-.090
Std. Error of Kurtosis		.254

PERF

	N	%
1.00	8	2.2%
1.50	1	0.3%

2.00	11	3.0%
2.50	7	1.9%
3.00	20	5.4%
3.50	25	6.8%
4.00	79	21.5%
4.50	38	10.3%
5.00	52	14.1%
5.50	26	7.1%
6.00	54	14.7%
6.50	21	5.7%
7.00	26	7.1%



Frequencies

Notes

Output Created		26-NOV-2020 20:43:31
Comments		
Input	Data	C:\Users\tfofu\Dropbox\ _NSU__ISEC- 0885_Doctoral_Research\ h\working\data\Computer Security Behaviors_2.sav
	Active Dataset	DataSet1
	File Label	File created by user 'asyncjobs_user' at Fri Oct 30 00:48:43 202
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	368
	Missing Value Handling	Definition of Missing
Cases Used		Statistics are based on all cases with valid data.

Syntax		FREQUENCIES VARIABLES=ATT /STATISTICS=SKEWNESS SESKEW KURTOSIS SEKURT /BARCHART FREQ /ORDER=ANALYSIS.
Resources	Processor Time	00:00:00.73
	Elapsed Time	00:00:00.32

Statistics

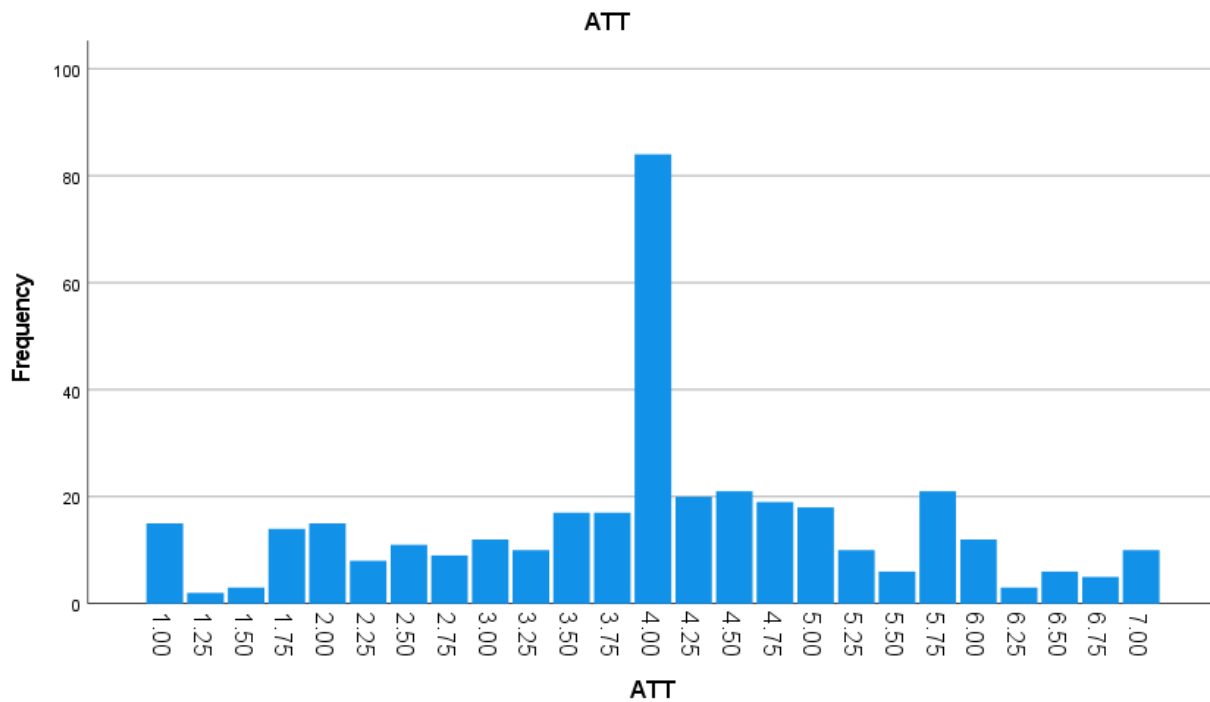
ATT

N	Valid	368
	Missing	0
Skewness		-.116
Std. Error of Skewness		.127
Kurtosis		-.260
Std. Error of Kurtosis		.254

ATT

	N	%
1.00	15	4.1%
1.25	2	0.5%

1.50	3	0.8%
1.75	14	3.8%
2.00	15	4.1%
2.25	8	2.2%
2.50	11	3.0%
2.75	9	2.4%
3.00	12	3.3%
3.25	10	2.7%
3.50	17	4.6%
3.75	17	4.6%
4.00	84	22.8%
4.25	20	5.4%
4.50	21	5.7%
4.75	19	5.2%
5.00	18	4.9%
5.25	10	2.7%
5.50	6	1.6%
5.75	21	5.7%
6.00	12	3.3%
6.25	3	0.8%
6.50	6	1.6%
6.75	5	1.4%
7.00	10	2.7%



OUTPUT MODIFY

Descriptives

Notes

Output Created	26-NOV-2020 20:46:26
Comments	
Input	Data
	C:\Users\tfofu\Dropbox\ _NSU__ISEC- 0885_Doctoral_Research\working\data\Computer Security Behaviors_2.sav
	Active Dataset
	DataSet1
	File Label
	File created by user 'asyncjobs_user' at Fri Oct 30 00:48:43 202

	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	368
Missing Value Handling	Definition of Missing	User defined missing values are treated as missing.
	Cases Used	All non-missing data are used.
Syntax		DESCRIPTIVES VARIABLES=ATT /STATISTICS=MEAN STDDEV MIN MAX KURTOSIS SKEWNESS.
Resources	Processor Time	00:00:00.02
	Elapsed Time	00:00:00.00

Descriptive Statistics

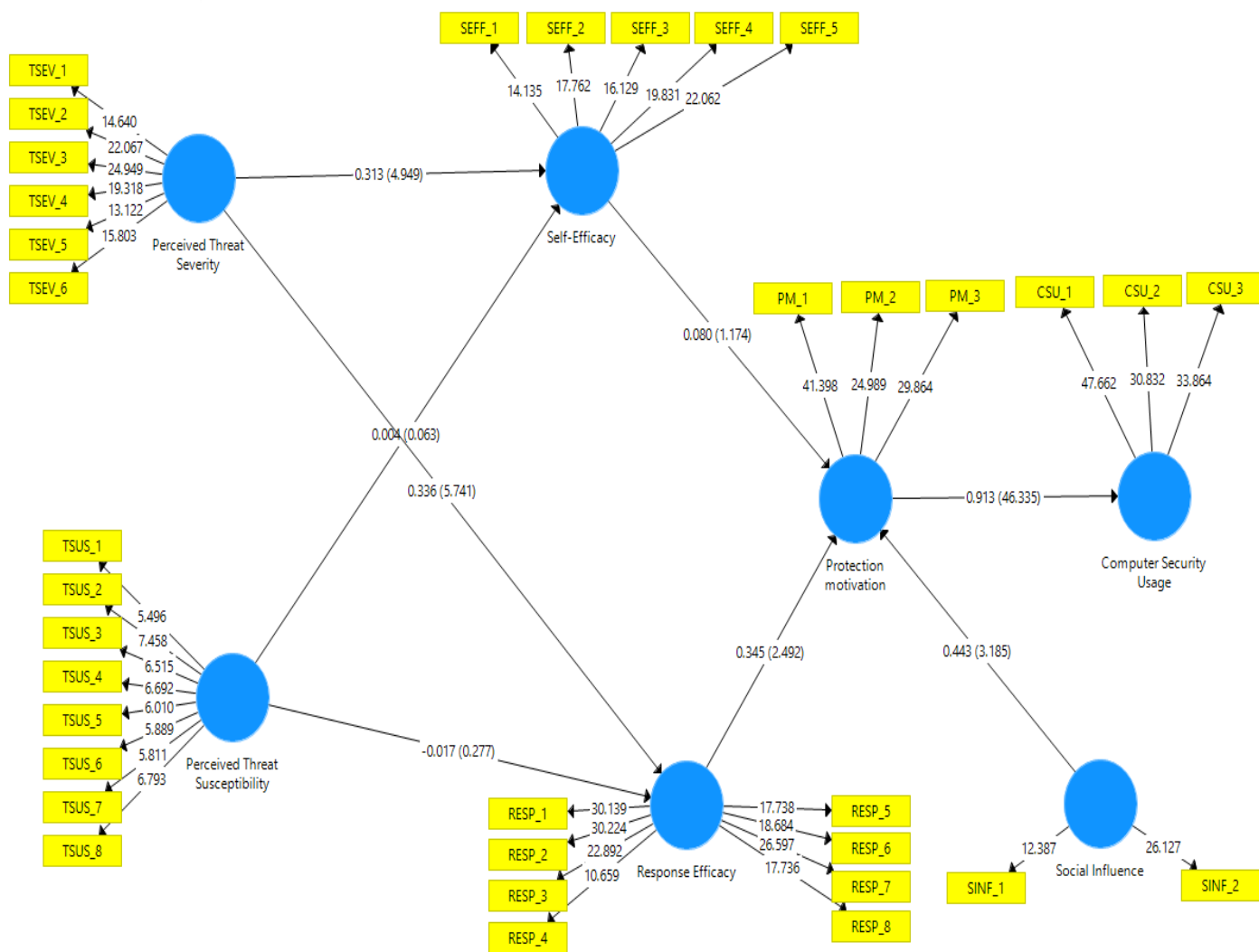
	N	Minimum	Maximum	Mean	Std. Deviation	Skewness	Std. Error
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic
ATT	368	1.00	7.00	4.0054	1.42297	-.116	.127
Valid N (listwise)	368						

Descriptive Statistics

	Kurtosis	
	Statistic	Std. Error
ATT	-.260	.254
Valid N (listwise)		

Appendix J:

Significance with Bootstrapping



Path Coefficients

Mean, STDEV, T-Values, P-Values	Confidence Intervals	Confidence Intervals Bias Corrected	Samples		
	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O /STDEV)	P Values
Perceived Threat Severity -> Response Efficacy	0.336	0.336	0.058	5.741	0.000
Perceived Threat Severity -> Self-Efficacy	0.313	0.316	0.063	4.949	0.000
Perceived Threat Susceptibility -> Response Efficacy	-0.017	-0.018	0.060	0.277	0.782
Perceived Threat Susceptibility -> Self-Efficacy	0.004	0.005	0.063	0.063	0.950
Protection motivation -> Computer Security Usage	0.913	0.914	0.020	46.335	0.000
Response Efficacy -> Protection motivation	0.345	0.339	0.138	2.492	0.013
Self-Efficacy -> Protection motivation	0.080	0.076	0.068	1.174	0.241
Social Influence -> Protection motivation	0.443	0.451	0.139	3.185	0.002

Path Coefficients

Mean, STDEV, T-Values, P-Values	Confidence Intervals	Confidence Intervals Bias Corrected	Samples		
	Original Sample (O)	Sample Mean (M)	2.5%	97.5%	
Perceived Threat Severity -> Response Efficacy	0.336	0.336	0.225	0.446	
Perceived Threat Severity -> Self-Efficacy	0.313	0.316	0.189	0.433	
Perceived Threat Susceptibility -> Response Efficacy	-0.017	-0.018	-0.143	0.087	
Perceived Threat Susceptibility -> Self-Efficacy	0.004	0.005	-0.113	0.133	
Protection motivation -> Computer Security Usage	0.913	0.914	0.872	0.950	
Response Efficacy -> Protection motivation	0.345	0.339	-0.004	0.575	
Self-Efficacy -> Protection motivation	0.080	0.076	-0.069	0.196	
Social Influence -> Protection motivation	0.443	0.451	0.230	0.785	

Total Effects

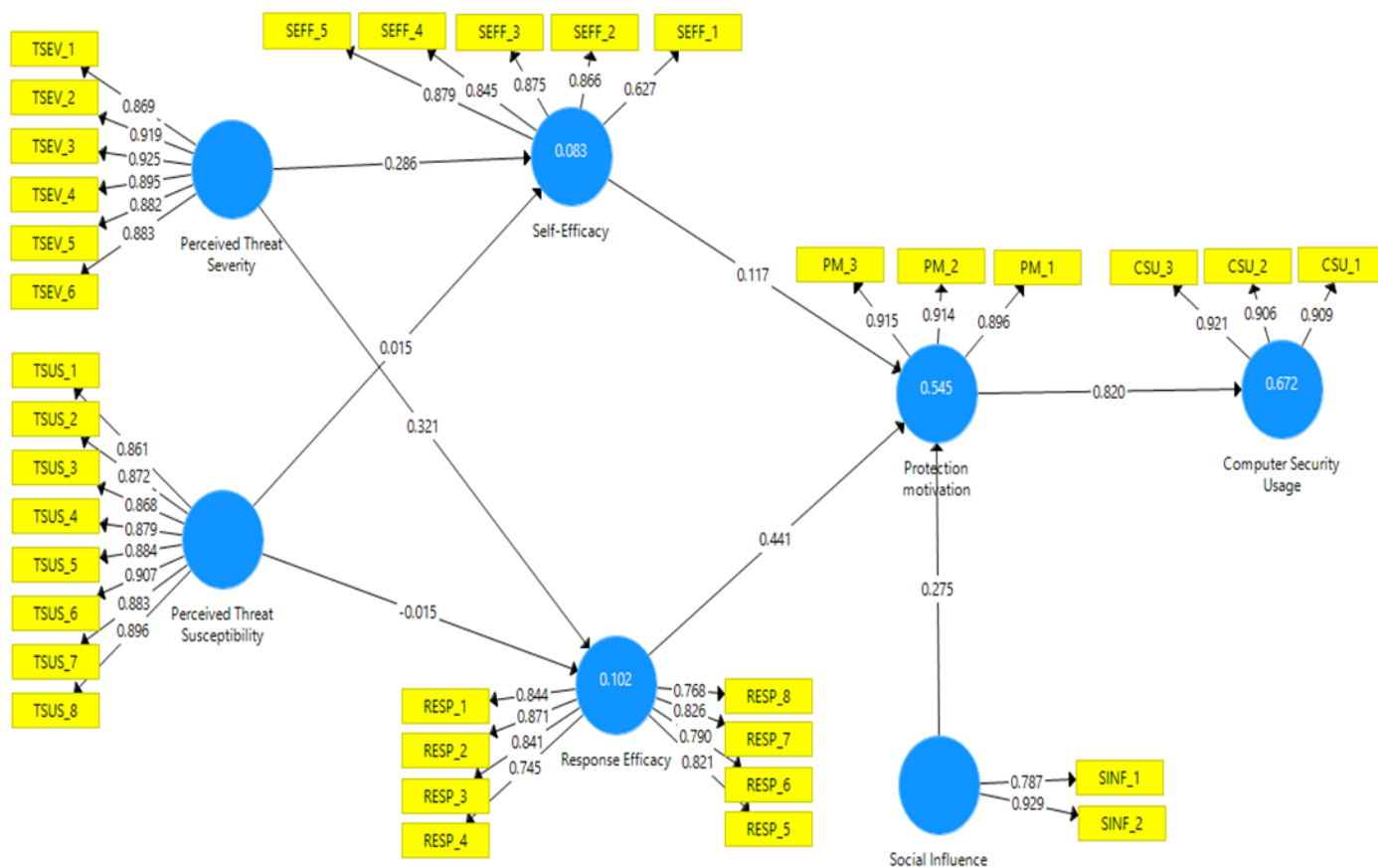
Mean, STDEV, T-Values, P-Values	Confidence Intervals	Confidence Intervals Bias Corrected	Samples		
	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O /STDEV)	P Values
Perceived Threat Severity -> Computer Security Usage	0.129	0.128	0.050	2.558	0.011
Perceived Threat Severity -> Protection motivation	0.141	0.139	0.054	2.588	0.010
Perceived Threat Severity -> Response Efficacy	0.336	0.336	0.058	5.741	0.000
Perceived Threat Severity -> Self-Efficacy	0.313	0.316	0.063	4.949	0.000
Perceived Threat Susceptibility -> Computer Security Usage	-0.005	-0.008	0.024	0.211	0.833
Perceived Threat Susceptibility -> Protection motivation	-0.005	-0.009	0.026	0.212	0.832
Perceived Threat Susceptibility -> Response Efficacy	-0.017	-0.018	0.060	0.277	0.782
Perceived Threat Susceptibility -> Self-Efficacy	0.004	0.005	0.063	0.063	0.950
Protection motivation -> Computer Security Usage	0.913	0.914	0.020	46.335	0.000
Response Efficacy -> Computer Security Usage	0.315	0.310	0.127	2.478	0.014
Response Efficacy -> Protection motivation	0.345	0.339	0.138	2.492	0.013
Self-Efficacy -> Computer Security Usage	0.073	0.069	0.063	1.171	0.242
Self-Efficacy -> Protection motivation	0.080	0.076	0.068	1.174	0.241
Social Influence -> Computer Security Usage	0.404	0.412	0.127	3.181	0.002
Social Influence -> Protection motivation	0.443	0.451	0.139	3.185	0.002

Total Effects

Mean, STDEV, T-Values, P-Values	Confidence Intervals	Confidence Intervals Bias Corrected	Samples		
	Original Sample ...	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O/STDEV)	P Values
Perceived Threat Severity -> Computer Security Usage	0.150	n/a	n/a		
Perceived Threat Severity -> Protection motivation	0.164	n/a	n/a		
Perceived Threat Severity -> Response Efficacy	0.340	n/a	n/a		
Perceived Threat Severity -> Self-Efficacy	0.312	n/a	n/a		
Perceived Threat Susceptibility -> Computer Security Usage	-0.005	n/a	n/a		
Perceived Threat Susceptibility -> Protection motivation	-0.006	n/a	n/a		
Perceived Threat Susceptibility -> Response Efficacy	-0.018	n/a	n/a		
Perceived Threat Susceptibility -> Self-Efficacy	0.014	n/a	n/a		
Protection motivation -> Computer Security Usage	0.913	n/a	n/a		
Response Efficacy -> Computer Security Usage	0.365	n/a	n/a		
Response Efficacy -> Protection motivation	0.400	n/a	n/a		
Self-Efficacy -> Computer Security Usage	0.082	n/a	n/a		
Self-Efficacy -> Protection motivation	0.090	n/a	n/a		
Social Influence -> Computer Security Usage	0.350	n/a	n/a		
Social Influence -> Protection motivation	0.383	n/a	n/a		

Appendix K:

PLS Analysis with Factor Loadings



Appendix L:

Survey



INSTITUTIONAL REVIEW BOARD
3301 College Avenue
Fort Lauderdale, Florida 33314-7796
PHONE: (954) 262-5369

**Participant Letter for Anonymous Surveys
NSU Consent to be in a Research Study Entitled**

Examination of the Computer Security Behaviors of Telecommuters Working with Confidential Data through Leveraging the Factors from Fear Appeals Model (FAM)

Who is doing this research study?

This person doing this study is Titus Dohnfon Fofung and a doctoral student at the College of Computing and Engineering at Nova Southeastern University. I will be helped by Dr. Ling Wang.

Why are you asking me to be in this research study?

You are being asked to take part in this research study because you are a telecommuter who works with sensitive or confidential data

Why is this research being done?

The purpose of this study is for my doctoral dissertation, I am conducting a research that seeks your anonymous input to a survey. The survey is to understand the factors that contribute to the information security behavior of telecommuters working with sensitive or confidential data in the context of data breach and spyware.

What will I be doing if I agree to be in this research study?

You will be taking a one-time, anonymous survey. The survey will take approximately 15 minutes or less to complete.

Are there possible risks and discomforts to me?

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.

What happens if I do not want to be in this research study?

You can decide not to participate in this research and it will not be held against you. You can exit the survey at any time.

Will it cost me anything? Will I get paid for being in the study?

There is no cost for participation in this study. Participation is voluntary and no payment will be provided.

How will you keep my information private?

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. Participant's information will be handled with rigorous



INSTITUTIONAL REVIEW BOARD
3301 College Avenue
Fort Lauderdale, Florida 33314-7796
PHONE: (954) 262-5369

confidentiality. SurveyMonkey utilizes servers that are strongly encrypted and reassures its users that all data is maintained secure and confidential. Ethical problems in the construction of the survey will be avoided, and the insertion of items that pursue personal data such as name and job title will not be included. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any granting agencies (if applicable). All confidential data will be kept securely on the researcher's home computer. All data will be kept for 36 months from the end of the study and destroyed after that time by deleting it from the home computer of the researcher and destroying the hard drive.

Who can I talk to about the study?

If you have questions, you can contact Titus Dohnfon Fofung at +1 404-983-7940. If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at IRB@nova.edu.

Do you understand and do you want to be in the study?

If you have read the above information and voluntarily wish to participate in this research study, please click on the "Next" button below on this page.

Next

DMG1	Gender
DMG 2	Age
DMG 3	Education
DMG 4	Computer experience
DMG 5	Work from home
DMG 6	Work with sensitive or confidential data
DMG 7	Installed anti-virus

Instrument

Computer Security Behaviors of Telecommuters Working with Confidential or Private Data

Demographics

1. What is your gender?

- Female
- Male

2. Select the interval that represents your year of birth.

- Silent Generation (1923 - 1944)
- Baby Boomer Generation (1946 - 1964)
- Generation X (1960 - 1980)
- Generation Y (1981 - 1994)
- Generation Z (1990 - 2002)

3. What is the highest level of education you have completed?

- High School
- Some College
- Bachelor's Degree
- Master's Degree
- Doctorate
- Other

4. How long have you been using a computer for work?

- < 6 months
- 6-12 months
- > 1 year to 2 years
- > 2 years to 3 years

> 3 years

5. Do you work from home?

Yes

No

6. Do you work with sensitive, private, or confidential data?

Yes

No

7. Do you have anti-virus installed on your computer?

Yes

No

Perceived Threat Severity

Please indicate the impact that each of these scenarios would have on you if it would occur.

8. My computer was infected by spyware.

Very Low Impact

Low Impact

Medium Low Impact

Medium Impact

Medium High Impact

High Impact

Very High Impact

9. My computer is becoming corrupted by a virus.

Very Low Impact

Low Impact

Medium Low Impact

Medium Impact

- Medium High Impact
- High Impact
- Very High Impact

10. My computer being taken over by a hacker.

- Very Low Impact
- Low Impact
- Medium Low Impact
- Medium Impact
- Medium High Impact
- High Impact
- Very High Impact

11. Sensitive data being stolen from my computer.

- Very Low Impact
- Low Impact
- Medium Low Impact
- Medium Impact
- Medium High Impact
- High Impact
- Very High Impact

12. Sensitive data being lost due to a virus on my computer.

- Very Low Impact
- Low Impact
- Medium Low Impact
- Medium Impact
- Medium High Impact
- High Impact
- Very High Impact

13. My computer is downloading a virus or an application with many bugs.

- Very Low Impact
- Low Impact
- Medium Low Impact
- Medium Impact
- Medium High Impact
- High Impact
- Very High Impact

Perceived Threat Susceptibility

Please indicate how likely you feel each scenario will occur with your computer.

14. My computer is at risk of becoming infected with spyware.

- Highly Unlikely
- Unlikely
- Somewhat Unlikely
- Neutral
- Somewhat Likely
- Likely
- Highly Likely

15. My computer will likely become infected with spyware.

- Highly Unlikely
- Unlikely
- Somewhat Unlikely
- Neutral
- Somewhat Likely
- Likely
- Highly Likely

16. My computer may become infected with spyware.

- Highly Unlikely

- Unlikely
- Somewhat Unlikely
- Neutral
- Somewhat Likely
- Likely
- Highly Likely

17. My computer becoming corrupted by a virus.

- Highly Unlikely
- Unlikely
- Somewhat Unlikely
- Neutral
- Somewhat Likely
- Likely
- Highly Likely

18. My computer being taken over by a hacker.

- Highly Unlikely
- Unlikely
- Somewhat Unlikely
- Neutral
- Somewhat Likely
- Likely
- Highly Likely

19. Sensitive or confidential data being stolen from my computer.

- Highly Unlikely
- Unlikely
- Somewhat Unlikely
- Neutral
- Somewhat Likely
- Likely

Highly Likely

20. Sensitive or confidential data is lost due to a virus on my computer.

Highly Unlikely

Unlikely

Somewhat Unlikely

Neutral

Somewhat Likely

Likely

Highly Likely

21. My computer is downloading a virus or an application with many bugs.

Highly Unlikely

Unlikely

Somewhat Unlikely

Neutral

Somewhat Likely

Likely

Highly Likely

Self-Efficacy

Please indicate the degree to which you agree or disagree with the following statements.

22. Using anti-spyware software increases my productivity.

Strongly Disagree

Disagree

Somewhat Disagree

Neither Agree nor Disagree

Somewhat Agree

- Agree
- Strongly Agree

23. I am confident about selecting the appropriate security software to use on my computer.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

24. I am confident about selecting the appropriate security settings on my computer.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

25. I am confident of correctly installing security software on my computer.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

26. I am confident of quickly finding information on using security software on my computer.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

Response Efficacy

Please indicate the degree to which you agree or disagree with the following statements.

27. Using anti-virus software works to protect my computer from a data breach.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

28. Using anti-malware software works to protect my computer from a data breach.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree

- Agree
- Strongly Agree

29. Using anti-virus software is effective in protecting my computer from a data breach.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

30. Using an anti-malware software is sufficient to protect my computer from a data breach.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

31. Using an anti-virus software would more likely protect my computer from a data breach.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

32. Using anti-malware software would more likely protect my computer from a data breach.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

33. Installation and frequent updates of anti-virus software is effective in preventing virus infections on my computer.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

34. If I install anti-virus software on my computer and update it frequently, I am less likely to have my system infected by a virus.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

Performance Expectancy

Please indicate the degree to which you agree or disagree with the following statements.

35. I find the use of anti-spyware software useful in my job.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

36. Using anti-spyware software enables me to accomplish tasks more quickly.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

Social Influence

Please indicate the degree to which you agree or disagree with the following statements.

37. People who influence my behavior think that I should use anti-spyware software.

- Strongly Disagree
- Disagree

- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

38. In general, my organization has supported using and providing anti-spyware software.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

Attitude

Please indicate the degree to which you agree or disagree with the following statements.

39. Anti-spyware software makes work more interesting.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

40. Working with anti-spyware software is fun.

- Strongly Disagree
- Disagree
- Somewhat Disagree

- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

41. I like working with anti-spyware software.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

42. Working with anti-spyware software is enjoyable.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

Protection Motivation

Please indicate the degree to which you agree or disagree with the following statements.

43. I am motivated to protect my computer from threats of a data breach.

- Strongly Disagree
- Disagree
- Somewhat Disagree

- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

44. I am motivated to prevent threats a data breach to my computer from being successful

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

45. I am motivated to engage in activities that protect my computer from threats of a data breach.

- Strongly Disagree
- Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree
- Agree
- Strongly Agree

Computer Security Usage

Please indicate the frequency you perform the following tasks.

46. I use firewall protection on my computer.

- Highly Unlikely
- Unlikely

- Somewhat Unlikely
- Neutral
- Somewhat Likely
- Likely
- Highly Likely

47. I use anti-virus software on my computer.

- Highly Unlikely
- Unlikely
- Somewhat Unlikely
- Neutral
- Somewhat Likely
- Likely
- Highly Likely

48. I use anti-malware software on my computer.

- Highly Unlikely
- Unlikely
- Somewhat Unlikely
- Neutral
- Somewhat Likely
- Likely
- Highly Likely

References

- Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology*, 78(2), 201-211.
- Ahn, J., & Jung, Y. (2016). The common sense of dependence on smartphone: A comparison between digital natives and digital immigrants. *New Media & Society*, 18(7), 1236-1256.
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613-643.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.
- Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, 36(1), 93-101.
- Al-Rawad, M. I., Al Khattab, A., Al-Shqairat, Z. I., Krishan, T. A., & Jarrar, M. H. (2015). An exploratory investigation of consumers' perceptions of the risks of online shopping in Jordan. *International Journal of Marketing Studies*, 7(1), 157-166.
- Altman, D. G., & Bland, J. M. (2005). Standard deviations and standard errors. *BMJ*, 331(7521), 903.
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312.
- Arora, S., Yttri, J., & Nilsen, W. (2014). Privacy and security in mobile health (mhealth) research. *Alcohol Research*, 36(1), 143150.
- Aurigemma, S., Mattson, T., & Leonard, L. (2017). So much promise, so little use: What is stopping home end-users from using password manager applications? Proceedings of 50th Hawaii International Conference on System Sciences, 4061– 4070.
- Bagozzi, R. P., & Fornell, C. (1982). Theoretical concepts, measurements, and meaning. *A Second Generation of Multivariate Analysis*, 2(2), 5-23.
- Bollen, K., & Lennox, R. (1991). Conventional wisdom on measurement: A structural equation perspective. *Psychological Bulletin*, 110(2), 305.
- Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864.

- Bernat, G., & Burns, A. (2000). An approach to symbolic worst-case execution time analysis. *IFAC Proceedings Volumes*, 33(7), 43-48.
- Boruff, J. T., & Storie, D. (2014). Mobile devices in medicine: a survey of how medical students, residents, and faculty use smartphones and other mobile devices to find information. *Journal of the Medical Library Association*, 102(1), 22.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.
- Byrne, B. M. (2001). *Structural equation modeling with AMOS*. Mahwah: Lawrence Erlbaum Associates.
- Chan, M., Woon, I., & Kankanhalli, A. (2006). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 1, 18-41.
- Chen, Y., Ramamurthy, K. R. & Wen, K.-W. (2013) Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems* 29, 157-188.
- Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, 295(2), 295-336.
- Chithambo, L. M. (2015). Security Concerns in Telecommuting within the Information Technology Industry. *Proceedings of Academic Forum Conference*, 53-64.
- Chowriwar, S. S., Mool, M. S., Sabale, P. P., Parpelli, S. S., & Sambhe, N. (2014). Mitigating denial-of-service attacks using secure service overlay model. *International Journal of Engineering Trends and Technology*, 8(9), 479-483.
- Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems*, 52(4), 20-29.
- Clements, J. A., Boyle, R., & Proudfoot, J. G. (2016). Exploring political skill and deception. *The International Journal of Sociology and Social Policy*, 36(3/4), 138-156.
- Cohen, J. (1992). Statistical power analysis. *Current Directions in Psychological Science*, 1(3), 98-101.
- Cohn, J. (1988). Statistical power analysis for the behavioral sciences. *Hillsdale, NJ: Lawrence Earlbam Associates*.

- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.
- D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), 43-69.
- Doane, A. N., Kelley, M. L., & Pearson, M. R. (2016). Reducing cyberbullying: A theory of reasoned action-based video prevention program for college students. *Aggressive Behavior*, 42(2), 136-146.
- Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2016). Who influences information security behaviours of young home computer users in Vietnam? An ego-centric network analysis approach. *Proceedings of Australasian Conference on Information Systems*, 281–297.
- Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8), 982-1003.
- Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research*, 38(2), 269-277.
- Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), 23.
- Du, H., Xu, H., Rosson, M. B., & Carroll, J. M. (2013, June). Effects of Fear appeals and point of reference on the persuasiveness of IT security communications. *Proceedings of International Conference on Intelligence and Security Informatics*, 82-84, IEEE.
- Dupuis, M. J., Crossler, R. E., & Endicott-Popovsky, B. (2016, January). Measuring the human factor in information security and privacy. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 3676-3685, IEEE.
- Edwards, K. (2015). *Examining the security awareness, information privacy, and the security behaviors of home computer users*. Nova Southeastern University.
- Faul, F., Erdfelder, E., Lang, A. G., & Buchner, A. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, 39(2), 175-191.
- Fenu, G., & Pau, P. L. (2015). An analysis of features and tendencies in mobile banking apps. *Procedia Computer Science*, 56, 26-33.

- Fil, T., & Ryan, C. (2014). *Computer and internet use in the United States*. US Department of Commerce, Economics and Statistics Administration, US Census Bureau.
- Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior* Reading, MA. Addison-Wesley. Ford, RC & Richardson, WD (1994). *Ethical decision making: A review of the empirical literature*. *Journal of Business Ethics*, 13, 205-221.
- Fox, A. K., & Royme, M. B. (2018). Private information in a social world: Assessing consumers' fear and understanding of social media privacy. *Journal of Marketing Theory and Practice*, 26(1-2), 72-89.
- Fry, R. B., & Prentice-Dunn, S. (2006). Effects of a psychosocial intervention on breast self-examination attitudes and behaviors. *Health Education Research*, 21(2), 287-295.
- Gay, L. R., Mills, G. E., & Airasian, P. W. (2009). *Educational research: Competencies for Analysis and Applications, Student Value Edition*. Upper Saddle River, NJ: Merrill.
- Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. *International Food and Agribusiness Management Review*, 21(3), 317-334.
- Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, 4(1), 7.
- Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information systems*, 16(1), 5.
- Gerhart, N., & Windsor, J. (2017). Cognitive stopping rules in a new online reality. *AIS Transactions on Replication Research*, 3(1), 2.
- Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2019). Empirical assessment of mobile device users' information security behavior towards data breach. *Journal of Intellectual Capital*.
- Graton, A., Ric, F., & Gonzalez, E. (2015). Reparation or reactance? The influence of guilt on reaction to persuasive communication. *Journal of Experimental Social Psychology*, 62, 40-49.
- 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.
- Guttek, B. A., & Winter, S. J. (1990). Computer use, control over computers, and job satisfaction. *People's Reactions to Technology, The Claremont Symposium on Applied Social Psychology*, (4), 121-144.

- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed, a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139-152.
- Han, B., Wu, Y., & Windsor, J. (2014). User's adoption of free third-party security apps. *The Journal of Computer Information Systems*, 54(3), 77-86.
- Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33(1), 2-16.
- Hartono, E., Holsapple, C. W., Kim, K. Y., Na, K. S., & Simpson, J. T. (2014). Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. *Decision Support Systems*, 62, 11-21.
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115-135.
- Hensher, D. A. (1987). Issues in the pre-analysis of panel data. *Transportation Research Part A: General*, 21(4-5), 265-285.
- Herath, T. & Rao, H. R. (2009a) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47, 154-165.
- Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.
- Hesse-Biber, S. N., & Leavy, P. (2011). Focus group interviews. *The Practice of Qualitative Research*, 163-192.
- Hohman, Z. P., Crano, W. D., & Niedbala, E. M. (2015). Attitude ambivalence, social norms, and behavioral intentions: Developing effective anti-tobacco persuasive communications. *Psychology of Addictive Behaviors*, 30(2), 209-219.
- Howell, D. C. (2012). *Statistical methods for psychology*. Belmont CA: Wadsworth Cengage Learning.
- Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, 49(2), 99-110.
- Hu, L.T., & Bentler, P.M. (1998). Fit Indices in covariance structure modeling: Sensitivity to under parameterized model misspecification. *Psychological Methods*, 3, 424-453.

- Iftode, F., & Pruna, C. S. (2014). Social influence for security. *Journal of Danubian Studies and Research*, 4(2).
- Howell, D. C. (2009). *Statistical methods for psychology*. Cengage Learning.
- Hox, J. J., Moerbeek, M., & Van de Schoot, R. (2017). *Multilevel analysis: Techniques and applications*. Routledge.
- Jansen, J., & Van Schaik, P. (2018). Persuading end users to act cautiously online: A fear appeals study on phishing. *Information & Computer Security*, 26(3), 264-276.
- Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, 20(2), 196-213.
- Jennings, E., Arlikatti, S., & Andrew, S. (2015). Determinants of emergency management decision support software technology: An empirical analysis of social influence in technology adoption. *Journal of Homeland Security & Emergency Management*, 12(3), 603-626.
- Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*, 50(2), 245-284.
- Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1), 113-134.
- Johnston, A.C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.
- Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, 71(12), 1163-1173.
- Kim, H. J., & Shin, W. (2018). The effects of message source and fear appeal on young adult's response to STD messages in Singapore. *Asian Journal of Communication*, 28(2), 185-204.
- Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information security. *Information Management & Computer Security*, 21(1), 5-15.

- Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems*, 25(2), 241-280.
- Laajasalo, T., Aronen, E. T., Saukkonen, S., Salmi, V., Aaltonen, M., & Kivivuori, J. (2016). To tell or not to tell? Psychopathic traits and response integrity in youth delinquency surveys. *Criminal Behaviour & Mental Health*, 26(2), 81-93.
- Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, 18(1), 4-13.
- Larsen, K. R., and Bong, C. H. (2016). A tool for addressing construct identity in literature reviews and Meta-analyses. *MIS Quarterly*, 40(3), 529-551.
- Lazarus, R. S., and Folkman, S. 1984. *Stress, Appraisal, and Coping*, New York: Springer Publishing.
- Lebek, B., Degirmenci, K., & Breitner, M. H. (2013, August). Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices. *Proceedings of the Nineteenth Americas Conference on Information Systems '13*, Chicago, Illinois, 15-17.
- Lee, Y., & Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management*, 45(2), 109-119.
- Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, 50(2), 361-369.
- Lewis W., Agarwal, R., and Sambamurthy, V. 2003. Sources of influence on beliefs about information technology use: An empirical study of knowledge workers. *MIS Quarterly*, 27(4), 657-678.
- Li, Q., & Clark, G. (2013). Mobile security: A look ahead. *IEEE Security & Privacy*, 11(1), 78-81.
- Li, H., & Sakamoto, Y. (2015). Re-tweet count matters: social influences on sharing of disaster-related tweets. *Journal of Homeland Security and Emergency Management*, 12(3), 737-761.
- Li, Y., & Siponen, M. T. (2011, July). A call for research on home users' information security behaviour. *Proceedings of Pacific Asia Conference on Information Systems*, 112.
- Lin, K. Y., & Lu, H. P. (2015). Predicting mobile social network acceptance based on mobile value and social influence. *Internet Research*, 25(1), 130-107.

- Loch, K. D., Straub, D. W., & Kamel, S. (2003). Diffusing the Internet in the Arab world: The role of social norms and technological cultururation. *IEEE Transactions on Engineering Management*, 50(1), 45-63.
- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469-479.
- Martin, F., & Ertzberger, J. (2013). Here and now mobile learning: An experimental study on The use of mobile technology. *Computers & Education*, 68, 76-85.
- McGill, T., & Thompson, H. (2017). Old Risks, New Challenges: Exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology*, 36 (11), 1111-1124.
- Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, 34(4), 1203-1230.
- Meroño-Cerdán, A. L. (2017). Perceived benefits of and barriers to the adoption of teleworking: peculiarities of Spanish family firms. *Behaviour & Information Technology*, 36(1), 63-74.
- Mertler, C., & Vannatta, R. (2013). *Advanced and multivariate statistical methods: Practical application and interpretation* (5th ed.). Glendale, CA: Pyrczak Publishing.
- Mertler, C. A., & Reinhart, R. V. (2016). *Advanced and multivariate statistical methods: Practical application and interpretation*. Taylor & Francis.
- Mills, A., & Sahi, N. (2019, January). An empirical study of home user intentions towards computer security. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 4864–4840.
- Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30(1), 106-143.
- Manogaran, G., Thota, C., Lopez, D., & Sundarasekar, R. (2017). Big data security intelligence for healthcare industry 4.0. *Cybersecurity for Industry 4.0*, 103-126.
- Moore, G. C., and Benbasat, I. 1991. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, 2(3), 192-222.
- Njoroge, K. S., & Mberia, H. (2014). Fear arousing persuasive communication: The use of threat and coping appraisal in breast cancer messages. *International Journal of Academic Research in Business and Social Sciences*, 4(10), 543.

- O'Keefe, D. J. (1990). Social judgment theory. *Persuasion: Theory and research*, 29-44.
- Oberheide, J., & Jahanian, F. (2010, February). When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments. *Proceedings of the 11th Workshop on Mobile Computing Systems & Applications*, Annapolis, Maryland, 43-48.
- Ögütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83-93.
- Orazi, D. C., & Pizzetti, M. (2015). Revisiting fear appeals: A structural re-inquiry of the protection motivation model. *International Journal of Research in Marketing*, 32(2), 223-225.
- Orazi, D. C., Warkentin, M., & Johnston, A. C. (2019). Integrating Construal-level Theory in Designing Fear Appeals in IS Security Research. *Communications of the Association for Information Systems*, 45(1), 22.
- Page, K. L., & Uncles, M. D. (2014). The complexity of surveying web participation. *Journal of Business Research*, 67(11), 2356-2367.
- Pahnila, S., Siponen, M., & Mahmood, A. (2007). Which factors explain employees' adherence to information security policies? An empirical study. *Proceedings of Pacific Asia Conference on Information Systems*, 73.
- Petersen, A. H., & Ekstrøm, C. T. (2019). dataMaid: Your Assistant for Documenting Supervised Data Quality Screening in R. *Journal of Statistical Software*, 90(1), 1-38.
- Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, 623-656.
- Plotnikoff, R. C., Lubans, D. R., Penfold, C. M., & Courneya, K. S. (2014). Testing the utility of three social-cognitive models for predicting objective and self-report physical activity in adults with type 2 diabetes. *British Journal of Health Psychology*, 19(2), 329-346.
- Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4), 179-214.
- Preacher, K. J., & Hayes, A. F. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior research methods, instruments, & computers*, 36(4), 717-731.
- Price, J. H., Daek, J. A., Murnan, J., Dimmig, J., & Akpanudo, S. (2005). Power analysis in survey research: Importance and use for health educators. *American Journal of Health Education*, 36(4), 202-209.

- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 758-778.
- Putwain, D., Remedios, R., & Symes, W. (2015). Fear appeals used prior high-stakes examinations: Why are they appraised as threatening and do they impact on subjective task value? *Learning and Instruction*, 40, 21-28.
- Reeder, R. W., Ion, I., & Consolvo, S. (2017). 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy*, 15(5), 55-64.
- Ringle, C. M., Wende, S., and Becker, J.-M. (2015). Smartpls 3. Boenningstedt: SmartPLS GmbH, <http://www.smartpls.com>.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change¹. *The Journal of Psychology*, 91(1), 93-114.
- Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology: A Sourcebook*, 153-176.
- Rovai, A. P., Baker, J. D., & Ponton, M. K. (2013). *Social science research design and statistics: A practitioner's guide to research methods and IBM SPSS*. Watertree Press LLC.
- Ruiter, R. A., Kessels, L. T., Peters, G. J. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology*, 49(2), 63-70.
- Sari, P. K., & Trianasari, N. (2014, May). Information security awareness measurement with confirmatory factor analysis. Proceedings of the *International Symposium on Technology Management and Emerging Technologies*, 218-223, IEEE.
- Saunders, M., Lewis, P., & Thornhill, A. (2003). Research methods for business students. *Essex: Prentice Hall: Financial Times*.
- Sekaran, U., & Bougie, R. (2013). *Research methods for business*. West Sussex, United Kingdom: John Wiley & Sons Ltd.
- Sharma, G., Shakya, S., & Kharel, P. (2014). Technology acceptance perspectives on user satisfaction and trust of e-government adoption. *Journal of Applied Sciences*, 14(9), 860-872.
- Shillair, R., Cotten, S. R., Tsai, H. S., Alhabash, S. LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, 199-207

- Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Quaternary Geochronology*, 49, 177-191.
- Siponen, M., Mahmood, M. A., & Pahlila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217-224.
- Siponen, M. T. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management & Computer Security*, 8, 197-209.
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 34(3), 503-522.
- Steelman, Z. R., Hammer, B. I., and Limayem, M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly*, 38(2), 355-378.
- Straub, D., Boudreau, M. C., and Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13, 380-427.
- Tabachnick, B. G., & Fidell, L. S. (2013). Using multivariate statistics: International edition. *Pearson2012*.
- Tan, M., & Aguilar, K. S. (2012). An investigation of students' perception of bluetooth security. *Information Management & Computer Security*, 20(5), 364-381.
- Taniguchi, A., Fujii, S., Azami, T., & Ishida, H. (2014). Persuasive communication aimed at public transportation-oriented residential choice and the promotion of public transport. *Transportation*, 41(1), 75-89.
- Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, 70, 376-391.
- Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: Toward a conceptual model of utilization. *MIS Quarterly*, 125-143.
- Tu, Z., & Yuan, Y. (2012, January). Understanding user's behaviors in coping with security threat of mobile devices loss and theft. *Proceedings of the 45th Hawaii International Conference of System Science*, Honolulu, Hawaii, 1393-1402.
- United States Census Bureau. (2015). American FactFinder - Results.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186-204.

- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478.
- Wall, J. D., & Warkentin, M. (2019). Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Information & Management*, 56(8), 103-157.
- Wang, E., Myers, M. D., & Sundaram, D. (2013). Digital natives and digital immigrants: Towards a model of digital fluency. *Business & Information Systems Engineering*, 5(6), 409-419.
- White, G. L. (2015). Education and prevention relationships on security incidents for home computers. *The Journal of Computer Information Systems*, 55(3), 29-37.
- White, G., Ekin, T., & Visinescu, L. (2017). Analysis of protective behavior and security incidents for home computers. *Journal of Computer Information Systems*, 57(4), 353-363.
- Williams, K. C. (2012). Fear appeal theory. *Research in Business and Economics Journal*, 5, 121.
- Willison, R., Warkentin, H., & Johnston, A. (2016). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, 28(2), 266-293.
- Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, 59(4), 329-349.
- Woods, S., Forsberg, C. W., Schwartz, E. C., Nazi, K. M., Hibbard, J. H., Houston, T. K., & Gerrity, M. (2017) The association of patient factors, digital access, and online behavior on sustained patient portal use: A prospective cohort of enrolled users. *Journal of Medical Internet Research*, 19(10), e345.
- Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *Proceedings of the 26th International Conference on Information Systems (ICIS)*, 367-380.
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799-2816.
- Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, 92, 36-46.
- Yildirim, E. (2016). The importance of information security awareness for the success of business enterprises. In: D. Nicholson D (ed). *Advances in Human Factors in Cybersecurity*. *Advances in Intelligent Systems and Computing*, 501. Springer.

- Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, 23(4), 407-415.
- Yu, J., Zo, H., Choi, M. K., & Ciganek, A. P. (2013). User acceptance of location-based social networking services: An extended perspective of perceived value. *Online Information Review*, 37(5), 711-730.
- Zhang, S., Gerhart, W. C. M., McLaughlin, A. C., & Allaire, J. C. (2017). Predicting computer proficiency in older adults. *Computers in Human Behavior*, 67, 106-112.