

2018

An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills

Carlene G. Blackwood-Brown

Nova Southeastern University, carlandos@yahoo.com

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

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

 Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

NSUWorks Citation

Carlene G. Blackwood-Brown. 2018. *An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1047)
https://nsuworks.nova.edu/gscis_etd/1047.

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

An Empirical Assessment of Senior Citizens' Cybersecurity Awareness,
Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and
Motivation to Acquire Cybersecurity Skills

by


Carlene Gail Blackwood-Brown

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2018

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



Yair Levy, Ph.D.
Chairperson of Dissertation Committee

5/31/2018
Date



John D'Arcy, Ph.D.
Dissertation Committee Member

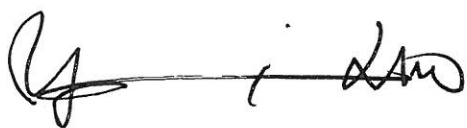
5/31/2018
Date



Ling Wang, Ph.D.
Dissertation Committee Member

5/31/2018
Date

Approved:



Yong X. Tao, Ph.D., P.E., FASME
Dean, College of Engineering and Computing

5/31/2018
Date

College of Engineering and Computing
Nova Southeastern University

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 Assessment of Senior Citizens' Cybersecurity Awareness,
Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and
Motivation to Acquire Cybersecurity Skills

by
Carlene Gail Blackwood-Brown
May 2018

Cyber-attacks on Internet users have caused billions of dollars in losses annually. Cyber-criminals launch attacks via threat vectors such as unsecured wireless networks and phishing attacks on Internet users who are usually not aware of such attacks. Senior citizens are one of the most vulnerable groups who are prone to cyber-attacks, and this is largely due to their limited cybersecurity awareness and skills. Within the last decade, there has been a significant increase in Internet usage among senior citizens. It was documented that senior citizens had the greatest rate of increase in Internet usage over all the other age groups during the past decade. However, whenever senior citizens use the Internet, they are being targeted and exploited particularly for financial crimes, with estimation that one in five becoming a victim of financial fraud, costing more than \$2.6 billion per year. Increasing the cybersecurity awareness and skills levels of Internet users have been recommended to mitigate the effects of cyber-attacks. However, it is unclear what motivates Internet users, particularly senior citizens, to acquire cybersecurity skills so that they can identify as well as mitigate the effects of the cyber-attacks. It is also not known how effective cybersecurity awareness training are on the cybersecurity skill level of senior citizens. Therefore, the main goal of this quantitative study was to empirically investigate the factors that contributed to senior citizens' motivation to acquire cybersecurity skills so that they would be able to identify and mitigate cyber-attacks, as well as assess their actual cybersecurity skills level. This was done by assessing a model of contributing factors identified in prior literature (senior citizens' cybersecurity awareness, computer self-efficacy, perceived risk of identity theft, & older adults' computer technology attitude) on the motivation of senior citizens to acquire cybersecurity skills. This study utilized a Web-based survey to measure the contributing factors and a hands-on scenarios-based iPad app called MyCyberSkills™ that was developed and empirically validated in prior research to measure the cybersecurity skills level of the senior citizens. All study measures were done before and after cybersecurity awareness training (pre- & post-test) to uncover if there were any differences on the assessed models and scores due to such treatment. The study included a sample of 254 senior citizens with a mean age of about 70 years.

Path analyses using Smart PLS 3.0 were done to assess the pre- and post-test models to determine the contributions of each contributing factor to senior citizens' motivation to acquire cybersecurity skills. Additionally, analysis of variance (ANOVA) and analysis of

covariance (ANCOVA) using SPSS were done to determine significant mean difference between the pre-and post-test levels of the senior citizens' cybersecurity skill level. The path analysis results indicate that while all paths on both models were significant, many of the paths had very low path coefficients, which in turn, indicated weak relationships among the assessed paths. However, although the path coefficients were lower than expected, the findings suggest that both intrinsic and extrinsic motivation, along with antecedents such as senior citizens' cybersecurity awareness, computer self-efficacy, perceived risk of identity theft, and older adults' computer technology attitude significantly impact the cybersecurity skill levels of senior citizens. The analysis of variance results indicated that there was a significant increase in the mean cybersecurity skills scores from 59.67% to 64.51% (N=254) as a result of the cybersecurity awareness training. Hence, the cybersecurity awareness training was effective in increasing the cybersecurity skill level of the senior citizens, and empowered them with small but significant improvement in the requisite skills to take mitigating actions against cyber-attacks. The analysis of covariance results indicated that, except for years using computers, all the other demographic indicators were not significant.

Contributions from this study add to the body of knowledge by providing empirical results on the factors that motivate senior citizens to acquire cybersecurity skills, and thus, may help in reducing some of the billions of dollars in losses accrued to them because of cyber-attacks. Senior citizens will also benefit in that they will be better able to identify and mitigate the effects of cyber-attacks should they attend cybersecurity awareness trainings. Additionally, the recommendations from this study can be useful to law enforcement and other agencies that work with senior citizens in reducing the number of cases relating to cybersecurity issues amongst senior citizens, and thus, free up resources to fight other sources of cybercrime for law enforcement agencies.

Acknowledgements

My first recognition, honor, adoration, praise, and gratitude go to my Lord and Saviour, Jesus Christ. My God has been with me at all times - He alone truly understands the struggles that I have been through on this journey, but amidst everything, I had the firm assurance of His love and provision. Therefore, through His wisdom and guidance from the Holy Spirit, I have overcome the obstacles to be the success I am today – thank you my God.

To my superb and supportive husband Orlando, along with our two wonderful and understanding boys, Te-Vaughn and Chrys-Brien, thank you for your “always guaranteed” continuous love and support. Orlando and boys, you did everything else for me so that I could focus on completing this journey – thank you for totally understanding in my times of absenteeism and for all the sacrifices you made to accommodate my studies – I love you all endlessly!

A very special thank you also to my very large (or, as we say in Jamaica, nuff nuff) extended family who has been my cheering team throughout the journey. Your words of encouragement, support, videos and jokes posted in our WhatsApp family chat kept me going on days when the workload seemed overwhelming – I have the best family – nuff luv, respect and big-up to all a oonu!

Dr. Yair Levy, my advisor – from the very first class that I had with you, I knew that I wanted to work with you. Many thought that I was crazy to approach you without a defined research problem, but deep down, I knew that I had to secure my spot early as you are considered first choice advisor by InfoSec students. Thankfully, you did not think I was crazy (or probably you did, but did not show it – LOL!), so you took me under your wings, and in the last three years, have given me top quality advice that cannot be labeled with a price tag. I could always look forward to your honest and professional feedback – as tough as some were, but in the end, I knew I could trust your judgement as you had my best interest at heart. Thank you for pushing me even when I doubted my capabilities – I recall wanting to take a stiff drink (although I do not drink) many times after our phone chats in which you would explain what is required – I knew I had to pull out my “A-game” as you would accept nothing less. Dr. Levy, you are simply the best – thank you!

Thank you also to my dissertation committee members: Dr. John D’Arcy and Dr. Ling Wang. I still think that it is surreal that the InfoSec research giant and expert, Dr. D’Arcy, has agreed to work with me – you can know that you are in an excellent position when the author of top-quality papers that you have referenced in your coursework assignments is working directly with you – life is great! Dr. Wang, a Quantitative Methods guru, caring, supportive, and understanding – the kind demeanor and professionalism that you displayed in the Quantitative Methods class that I took with you continued in my dissertation process. I am very grateful and appreciative of the valuable, timely, and excellent feedback that you both have given following the reviews of my submissions. I

am convinced that the make-up of my dissertation committee is a match made in heaven, and the outcome can only be excellence!

A huge thank you to all who worked with me in getting participants and a place to conduct the training for my study: Elisabete Way and the team at the LIFE Institute, Ryerson University, Canada; Dr. Andrew Isaacs and the team in the Faculty of Engineering and Computing at the University of Technology, Jamaica; Linda Maurice and the team at the Lifelong Learning Institute at Nova Southeastern University, Florida; Levenle Jean-Joseph and the team in the College of Engineering and Computing at Nova Southeastern University, Florida; Pastor Frank Douglas and the leadership team at North Park Worship Center, Canada; Galit Shemesh and the team at The Michael-Ann Russell Jewish Center, Florida, and the many families and friends who promoted my study and encouraged participation. To get participants who are 60 years or older who use the Internet to participate in a three-part study was no easy task – thank you!

To my wonderful and energetic 254 senior citizens who completed all three parts of my study: Words are inadequate to express my sincere gratitude to you for your interest and willingness to participate in my study. Committing to participation could not have been easy as you had to do a lengthy pre-and-post-test, plus attend a 2-hr face-to-face training session, which, in a lot of cases were miles away from your homes, and in adverse winter conditions. Your vibrancy, keen interest, and eagerness to learn about cybersecurity was a huge motivation to me – I always looked forward to our interesting discussions in the training sessions – thank you!

Lastly, to my friends, colleagues, and students at Seneca College as well as Sheridan College who supported and cheered me on throughout the process – thank you!

May God bless you all!

Dedication

I dedicate the efforts and results of my educational journey to my parents (deceased), my siblings, my husband, and my children.

To my parents, Arthur and Sybil Blackwood: My heart breaks to know that you are not here to celebrate with your last child of 13, i.e. your “wash-belly” on achieving this milestone, but I can imagine you both in heaven ‘a mek nuff noise’ in celebration with me as I walk the stage. Your upbringing, love, support, and example of reliance on God gave me the start as well as built a strong foundation on which I could build my life.

To my eight brothers, James, Dalton, Josiah, Radcliff, Gilbert, Herchell, Garfield, and Paul, along with my four sisters, Cynthia, Verolyn, Arthurine, and Jennifer: Every one of you have contributed to my journey and development – you all pitched in and took care of me, the “wash belly” when mom and dad could not afford to. You supported and pushed me to go to places that you did not go, without displaying an ounce of grudge – I really wanted to do this for you all, and I hope that I represent you well.

To my amazing husband, Orlando: You joined our family and continued the love and support that I had gotten so used to – some may say that I am spoiled, but naah, I don’t so. With your selfless love and continuous support, you deserve this achievement as much as I do.

To my blessings, my wonderful children, Te-Vaughn and Chrys-Brien: Continue to ask God for direction, find your passion, take the first step towards it, stay focused, and one day you will reap the benefits of your dedication. Always remember that it is not only about how you start, but more so, about how you finish.

Table of Contents

Abstract	ii
Acknowledgements	iv
Dedication	vi
List of Tables	x
List of Figures	xi

Chapters

1. Introduction 1

Background	1
Problem Statement	2
Dissertation Goal	8
Research Questions and Propositions	15
Relevance and Significance	18
Relevance	18
Significance	19
Barriers and Issues	19
Limitations and Delimitations	20
Limitations	20
Delimitations	21
Definition of Terms	22
Summary	25

2. Literature Review 28

Introduction	28
Theoretical Foundation – Motivation	28
Intrinsic and Extrinsic Motivation	35
Cybersecurity	43
Definition and Importance	43
Cybersecurity Threats and Cyber-Attacks	46
Cyber-attack Vectors	51
Cybersecurity Awareness	55
Cybersecurity Skills	61
Risk and Risk Mitigation	65
Definition and Types of Risk	65
Perceived Risk	66
Perceived Risk of Identity Theft	77
Computer Self-Efficacy	81
Older Adults' Computer Technology Attitude	88
Senior Citizens' Use of Computers	94
Role of Demographic Variables in Cybersecurity	99
Summary of What is Known and Unknown in Research Literature	105

3. Methodology 107

- Research Design 107
- Survey Instrument and Measures 109
 - Expert Panel 113
 - Pilot Test 114
 - MyCyberSkills™ iPad app 115
 - Instrument Validity and Reliability 117
 - Internal Validity 119
 - External Validity 121
 - Specific Research Steps 121
- Population and Sample 124
- Pre-analysis Data Screening 124
- Data Analysis 126
 - Data Aggregation 128
- Resources 128
- Summary 129

4. Results 130

- Overview 130
- Phase One – Validation Procedures for Survey Instrument 130
 - Expert Panel 131
- Phase Two – Pilot Test 132
- Phase Three – Main Data Collection 133
 - Main Data Collection Procedures 133
 - Pre-analysis Data Screening 137
 - Demographic Analysis 138
 - Reliability and Validity 140
- Research Questions and Propositions 142
 - Proposition Testing 144
- Summary 149

5. Conclusion, Implications, Recommendations, and Summary 151

- Conclusions 151
- Discussion 152
 - Proposition 1_(a & b) 153
 - Proposition 2_(a & b) 154
 - Proposition 3_(a & b) 156
 - Proposition 4_(a & b) 157
 - Proposition 5_(a & b) 158
 - Assessment of R² Values 160
 - Proposition 6_(a & b) 163
 - Proposition 7_(a to h) 164
- Limitations of the Study 165
- Future Research 166
- Implications and Recommendations 167

Theoretical Implications 167
Practical Implications 168
Summary 170

Appendices

A. Institutional Review Board Approval Letter 178
B. Instrument for Participants 179
C. Expert Panel Recruitment Email 199
D. Expert Panel Questionnaire with Proposed Instrument 201
E. Pilot Test Solicitation Letter 221
F. Pilot Test Questionnaire with Instrument 223
G. Participant Email 243

References 245

List of Tables

Tables

1. Summary of Motivation-related (Intrinsic & Extrinsic) Literature 36
2. Summary of Cybersecurity-related Literature 45
3. Summary of Cybersecurity Threats and Cyber-Attacks Literature 49
4. Summary of Cyber-Attack Vectors Literature 53
5. Summary of Cybersecurity Awareness-related Literature 58
6. Summary of Cybersecurity Skills-related Literature 63
7. Summary of Perceived Risks-related Literature 71
8. Summary of Perceived Risk of Identity Theft-related Literature 79
9. Summary of CSE-related Literature 82
10. Summary of Older Adults Computer Technology Attitude-related Literature 91
11. Summary of Senior Citizens' Use of Computer-related Literature 96
12. Summary of the Role of Demographic Variables in Cybersecurity-related Literature 102
13. Descriptive Statistics of the Population (N=254) 139
14. Reliability (Cronbach's Alpha) and Validity (AVE) for This Study's Constructs 141
15. Summary of Proposition Testing for P1 to P5 (N=254) 146
16. ANCOVA: Tests of Between-Subjects Effects - Dependent Variable: CyberSkills (N=254) 148

List of Figures

Figures

1. Research Model for Factors that Contribute to Senior Citizen's Motivation to Acquire Cybersecurity Skills 17
2. Research Study Methodology 108
3. Outcome of the PLS Pre-Test Paths 143
4. Outcome of the PLS Post-Test Paths 144
5. Pre-and-Post-Test CyberSkills Score Means (N=254) 147

Chapter 1

Introduction

Background

Cyber-attacks that exploit human vulnerabilities are constantly evolving, and as such, billions of dollars in losses have been accrued to Internet users (Abawajy, 2014). For example, phishing directly targets humans by circumventing the cybersecurity measures that they have in place, and that can lead to damaging losses, including, but not limited to, identity theft (Hong, 2012). Senior citizens are one of the most vulnerable groups of Internet users who are prone to cyber-attacks, and this results from the fact that they have limited cybersecurity awareness and skills (Claar & Johnson, 2012; Grimes, Hough, Mazur, & Signorella, 2010). Therefore, cybersecurity awareness is essential for senior citizens as a countermeasure strategy to combat the cyber-attacks that they face (Choo, 2011). According to Rahim, Hamid, Kiah, Shamshirband, and Furnell (2015), cybersecurity awareness involves “alerting Internet users of cybersecurity issues and threats, and enhancing Internet users’ understanding of cyber threats so they can be fully committed to embracing security during Internet use” (p. 607). However, despite the losses caused by cyber-attacks, it appears that it is still unclear what motivates Internet users, more so senior citizens, to acquire cybersecurity skills so that they will be able to identify cyber-attacks as well as mitigate the effects of those attacks when they use the Internet (Grimes et al., 2010; Lam & Lee, 2006; Ng, 2007; Shillair, Cotten, Tsai,

Alhabash, LaRose, & Rifon, 2015). This study empirically assessed the factors that contributed to senior citizens' motivation to acquire cybersecurity skills, as well as assessed their actual cybersecurity skills levels using a previously developed and validated scenario-based iPad application (Carlton & Levy, 2015; Carlton, Levy, Ramim, & Terrell, 2016). The findings from this study provided empirical results on the factors that motivate senior citizens to acquire cybersecurity skills so that they can identify and mitigate the effects of cyber-attacks. Additionally, the findings support prior claims that cybersecurity awareness training is effective in increasing cybersecurity skills levels (Albrechtsen & Hovden, 2010; D'Arcy, Hovav, & Galletta, 2009; Kritzinger & von Solms, 2010; Rahim et al., 2015)

Problem Statement

The problem that this research addressed is the increase in the success of cyber-attack vectors due to limited cybersecurity awareness and skills among Internet users, especially senior citizens, which ultimately causes them significant financial losses (Abbasi, Zhang, Zimbra, Chen, & Nunamaker, 2010; D'Arcy et al., 2009; Purkait, Kumar De, & Suar, 2014). According to Lemoudden, Bouazza, El Ouahidi, and Bourget (2013), an attack vector is a path through which a cyber-criminal can gain access to a network server or a computer to deliver a malicious code or obtain information for malicious purposes. Attack vectors such as unsecured wireless (Wi-Fi) networks and phishing attacks are the most common ways for cyber penetrations to happen (Futcher, 2015; Noor & Hassan, 2013). Aïmeur and Schonfeld (2011) warned Wi-Fi users against accessing services that were of a sensitive nature, for example, financial services, via public Wi-Fi

networks because those networks were often unsecured, and would leave the users exposed to cyber-attacks. However, a recent Symantec Corporation Report indicated that such warning had gone unheeded. For example, in 2013, a survey of 13,022 adults revealed the following about Wi-Fi users' actions on unsecured Wi-Fi networks: 56% accessed their social network account, 54% accessed personal e-mail, 29% accessed their bank account, 29% shopped online, three out of 10 did not always log off after having used a public Wi-Fi connection, and 39% did not take any special steps to protect themselves when using public Wi-Fi networks (Symantec, Norton Report, 2013). Similar to the use of unsecured Wi-Fi networks, phishing attacks on Internet users can also pose serious threats to their private lives, including, but not limited to compromising of confidential information, and identity theft (Akopyan & Yelyakov, 2009). Choo (2011) defined phishing as:

Online scams that frequently use unsolicited messages purporting to originate from legitimate organizations, particularly banking and finance services, to deceive victims into disclosing their financial and/or personal identity information (PII) to commit or facilitate other crimes (e.g. fraud, identity theft and theft of sensitive information). (p. 724)

PII refers to information that can be used to identify or locate a person, for example, name, address, phone number, email address, fax number, credit card number or Social Security number (Federal Trade Commission [FTC], 2000). Identity theft is a crime that occurs when a person unlawfully uses another person's PII for personal gain, for example, to obtain financial benefits, or, with the intention to commit fraud or other crimes (Bellah, 2001; Lai, Li, & Hsieh, 2012). Abbasi et al. (2010) as well as Jansson and

von Solms (2013) claimed that there was an increase in phishing attacks, and that could result in billions of dollars in fraudulent revenues at the expense of Internet users who were not aware of those types of attacks. In 2014, there were 163,333 submitted incidents of phishing attacks during quarter three, while in quarter four, there were 197,252 submitted incidences (Anti-Phishing Working Group, 2015). This represented a 20% increase over the two quarters of the same year. The aforementioned evidences suggest that unsecured Wi-Fi networks and phishing attacks continue to be threat vectors through which cyber-criminals can attack Internet users. Therefore, more work is needed in these areas to make Internet users, including home computer users (HCUs) aware of the potential dangers of such attack vectors, as well as to develop the skills on how to mitigate the impacts of cyber-attacks. According to Kritzinger and von Solms (2010), a home computer user (HCU) is a person who accesses the Internet from a personal computer for personal use outside the work environment, and is self-responsible to secure the computer in terms of malware protection, updates, patches etc. Iyer and Eastman (2006) stated that senior citizens make up one of the fastest growing groups of Internet users. Such statement still holds true as over the last decade, evidence shows that there has been a significant increase in Internet usage by American senior citizens over all other age groups that were surveyed. The Pew Research Center conducted 97 surveys and interviewed over 229,000 Internet users between 2000 and 2015. The 2005 results indicated that at the two ends of the age spectrum, Internet usage amongst senior citizens was 28%, while it was 83% amongst the 18-29 age group. A decade later, the 2015 results indicated that the usage had risen to 58% amongst senior citizens, while it rose to 96% amongst the 18-29 age group (Perrin & Duggan, 2015). This means that senior

citizens had a greater rate of increase in Internet usage (107% increase) over the 18–29 age group (16% increase) for the same period. According to Willis (2015), senior citizens were being targeted and exploited over the Internet, with one in five American senior citizens being a victim of financial fraud, costing more than \$2.6 billion per year. Jones (2001) indicated that after having their identity stolen via Internet use, some senior citizens suffered devastating effects, ranging from loss of all their life savings, feelings of shame for being victims, and exacerbated illnesses, to include premature death. Identity theft is, therefore, one of the common fears of senior citizens when they use the Internet (Jones, 2001). This fear, coupled with their limited cybersecurity awareness and skills, cause them to feel overwhelmed, frustrated as well as demotivated when they use the Internet (Greengard, 2009; Jones, 2001). Iyer and Eastman (2006) also reported that senior citizens who were not satisfied with their cybersecurity skills levels would have less confidence in their abilities to use the Internet for personal use such as communication, entertainment, shopping, and banking. There have been calls from several researchers regarding the issue of increasing the awareness of cybersecurity countermeasures of Internet users. In their call, Mensch and Wilkie (2011) stated that Internet users should take proactive cybersecurity countermeasures, as well as to stay up-to-date on the available cybersecurity tools and procedures that could protect their personal data. However, the Mensch and Wilkie (2011) study focused on college students who had access to training provided by the college, and hence did not face the same issues as other HCU. Jones and Heinrichs (2012) as well as White (2015) also recommended that Internet users should increase their cybersecurity awareness in order to acquire the skills to counter the dangers of cyber-attacks. Shapira, Barak, and Gal

(2007) reported that senior citizens with higher levels of cybersecurity awareness were motivated to use the Internet as they would experience increased self-efficacy, and displayed enthusiasm because they were better able to counter cyber-attacks. A motivated person is someone who is energized, enthused, and inspired to perform an activity, while an unmotivated person is someone who performs an activity without inspiration or enthusiasm (Ryan & Deci, 2000). Contrary to the findings of Shapira et al. (2007), Paine, Reips, Stiegerc, Joinsona, and Buchanand (2007) reported that even with the necessary skills, if senior citizens perceived that they were at risks of cyber-attacks, example, identity theft, they would be less motivated to use the Internet. Nemati and Van Dyke (2009) defined perceived risk as “a person’s belief in the likelihood that they will be harmed as a consequence of taking a particular action” (p. 52). For example, some senior citizens felt that when they divulged sensitive information such as PII on the Internet, they were at greater risk of identity theft, therefore, in those circumstances, they were less motivated to use the Internet (Morgan & Ravindran, 2014; Paine et al., 2007). Johnston and Warkentin (2010) on the other hand, found that when users perceived that they were at risk of cyber-attacks, they were more motivated and aware when they use the Internet. Therefore, further investigation is required into the mixed conclusions regarding the reasons Internet users, especially senior citizens, are motivated to use the Internet, given perceptions of risks. Further, the attitude that senior citizens have towards using technology such as the Internet can motivate their actions towards the use of the technology (Laganá, Oliver, Ainsworth, & Edwards, 2011; Regan & Fazio, 1977). Chen and Chan (2013) as well as Schmidt, Wahl, and Plischke (2014) indicated that contrary to previously held beliefs, senior citizens had an overall positive attitude towards

technology. Positive computer attitudes were related to convenience of use such as making activities easier and faster, while negative attitudes were related to health risks as well as social problems such as addiction and social isolation (Chen & Chan, 2013). Negative attitudes towards computers will ultimately affect an individual's motivation to using computers (Levine Donitsa-Schmidt, 1998). Therefore, since senior citizens' technological actions were likely to be guided by their attitudes, enhancing their technological attitudes should lead to increasing the use of new and emerging technologies (Laganá et al., 2011). Anderson and Agarwal (2010) stated that reports in the literature have placed less attention on investigating cybersecurity awareness issues from the perspective of HCUs. In response, Grimes et al. (2010) conducted a study that focused on the levels of cybersecurity awareness of senior citizens who accessed the Internet in unsecured Wi-Fi settings, such as, at home, libraries, mall, coffee shops, and senior centers. Grimes et al. (2010) concluded that further research was necessary to determine what types of cybersecurity awareness training would be most effective in training senior citizens who had limited cybersecurity awareness and skills. In light of the aforementioned studies, it appears that the literature has limited research reported regarding the cybersecurity issues from the perspective of HCUs, especially senior citizens. Therefore, additional empirical investigation into reducing the success of cyber-attacks vectors that result from limited cybersecurity awareness and skills among Internet users appears to be warranted.

Dissertation Goal

The main goal of this research study was to empirically assess the contributions of senior citizens' cybersecurity awareness (SCCA), computer self-efficacy (CSE), perceived risk of identity theft (PRIT), and older adults' computer technology attitude (OACTA) on their motivation (intrinsic [IM] & extrinsic [EM]) to acquire cybersecurity skills, as well as their cybersecurity skill (CyberSkills) level, while comparing each before and after cybersecurity awareness training. According to Shillair et al. (2015), Internet users need to be motivated before they commit to cybersecurity countermeasures because extra effort is required. Deci (1971) distinguished between the two types of motivation (intrinsic & extrinsic), based on the different reasons that caused a person to perform an activity or action. According to Deci (1971):

A person is intrinsically motivated if he performs an activity for no apparent reward except the activity itself. Extrinsic motivation, on the other hand, refers to the performance of an activity because it leads to external rewards (e.g., status, approval, or passing grades). (p. 113)

Since intrinsic motivation occurs when a person performs an activity simply for the enjoyment of it, the person would be more willing to devote extra time and effort to the activity being performed (Lee, Lee, & Hwang, 2015). Moon and Kim (2001), as well as Venkatesh and Davis (2000) indicated that both intrinsic and extrinsic motivation contributed to a user's positive experience with computers. Within the context of using the Internet, Teo, Lim, and Lai (1999) also found that both intrinsic and extrinsic motivation played positive roles in participants' Internet usage. However, the aforementioned studies were conducted within a workplace context and while the

findings were consistent, there were no indications if those or similar findings would hold true for HCUs, especially senior citizens. Slegers, van Boxtel, and Jolles (2012) asserted that as a result of the benefits that senior citizens got from using the Internet, they may feel intrinsically rewarded, which may ultimately motivate them to continue using the Internet. However, Slegers et al. (2012) did not measure motivation, nor was it proven in their study, therefore, this assertion is inconclusive. Lam and Lee (2006) noted that among Internet users, senior citizens was a distinct group that required separate consideration for training because they had different characteristics and faced challenges that were not the same as, for example, Internet users in the workplace. Some of the challenges faced by senior citizens due to their age can be cognitive as well as physical, such as fading memory, slower speed at processing information, poor vision, and slow motor skills resulting from chronic conditions (Greengard, 2009). In light of the separate consideration required for senior citizens, Lam and Lee (2006) conducted a three-part longitudinal study (over a period of one year) that focused on training senior citizens in basic uses of the computer and the Internet. Overall, the results from the Lam and Lee (2006) study indicated that the training program improved the psychological state of mind of the senior citizens, which manifested in increased self-efficacy, and they were intrinsically motivated to pursue additional training to improve their skills. However, Ng (2007) reported that key challenges for senior citizens were motivating them to develop new computing skills, and once the skills were developed, to keep on practicing them. The results from the Ng (2007) study showed that senior citizens could be motivated to acquire skills to use technology when social elements such as interactions with their peers were embedded in the training programs. Further, Hart, Chaparro, and Halcomb (2008)

reported that senior citizens would be motivated to use the Internet if they perceived it to be useful, beneficial, and that it provided enrichment to their quality of life. However, the training programs in the previous studies (Hart et al., 2008; Lam & Lee, 2006; Ng, 2007) focused mainly on general and basic computer uses, without direct focus on increasing cybersecurity skills to counter cyber-attacks. Similar criticisms were made by Grimes et al. (2010) who stated that most of the research on senior citizens' computer use had only focused on issues such as basic computer knowledge, and benefits of computer use. Additionally, the aforementioned studies did not measure the motivation levels of the senior citizens to acquire cybersecurity skills. Such gaps were addressed in this research study as the contributions of senior citizens' SCCA, CSE, PRIT, and OACTA on their motivation (IM & EM) to acquire cybersecurity skills, as well as their CyberSkills level, while comparing each before, and after cybersecurity awareness training, were measured as well as discussed.

The need for this work was demonstrated by the work of Shillair et al. (2015) who found that despite widespread warnings of the dangers of having limited cybersecurity awareness and skills, a large percentage of Internet users was still very naïve about cybersecurity. Therefore, Shillair et al. (2015) recommended that cybersecurity awareness training should be given to Internet users to develop skills to counter cyber-attacks. Shillair et al. (2015) also indicated that cybersecurity awareness training would increase the self-efficacy levels of the Internet users, and they would be motivated to expend the effort necessary to counter those attacks. Moreover, the need for this work is also demonstrated by the work of Carlton and Levy (2015) who assessed the top platform independent cybersecurity skills of non-information technology (IT) professionals. Their

results identified the prevention of PII theft via access to unsecured networks, and preventing PII theft via email phishing among the top nine cybersecurity skills that were needed by non-IT professionals to counter cyber-attacks. Ramim and Levy (2006) as well as Abawajy (2014), reported that one of the biggest challenges in cybersecurity was the limited cybersecurity skills of Internet users. Skill is a combination of knowledge, experience, and ability that enabled end-users to perform a task well (Boyatzis & Kolb, 1991; Levy, 2005). Carlton and Levy (2015) stated that “cybersecurity skills correspond to an individual’s technical knowledge, ability, and experience surrounding the hardware and software required to execute information security in protecting their IT against damage, unauthorized use, modification, and/or exploitation” (p. 3). The work of Shillair et al. (2015), along with the results from the Carlton and Levy (2015) study, imply that specific cybersecurity awareness training is required to develop the cybersecurity skills levels of users to counter cyber-attacks. According to Kruger and Kearney (2008), cybersecurity awareness training programs were most effective when the training material and activities directly addressed specific cybersecurity needs, as well as, were monitored. Thus, training non-IT professionals such as senior citizens on countermeasures against specific cyber-attacks such as PII theft when using Wi-Fi networks, as well as emails should be effective to address the needs identified in the Shillair et al. (2015), as well as the Carlton and Levy (2015) studies. Additionally, this type of focused training, both of content and target group, will address the limitations identified in the Hart et al. (2008), Lam and Lee (2006), as well as the Ng (2007) studies. In 2010, when the Internet usage among senior citizens in the US was 43%, Grimes et al. (2010) emphasized that it was crucial to assess whether senior citizens who use the

Internet were aware of cyber-attacks, and to what extent their limited awareness would place them at greater risk of cyber-attacks. Such limited awareness of cybersecurity countermeasures would increase the senior citizens' perceptions of risks, and actual vulnerability to cyber-attacks. With the increased Internet usage of senior citizens, there is now more urgency to address the call made by Grimes et al. (2010). Reisig, Pratt, and Holtfreter (2009) found that there were high levels of perceived risks among senior citizens when they used their credit cards online, which resulted in them spending less time on the Internet. Reisig et al. (2009), therefore, suggested that further research on the perceived risk of other online victimizations such as identity theft among senior citizens be conducted. Malhotra, Kim, and Agarwal (2004) found that in cases where Internet users had privacy concerns when using the Internet, there was a reduction in trust and an increase in perceptions of risks, resulting in reduced use of the Internet, especially, e-commerce sites. The studies of Malhotra et al. (2004) and Reisig et al. (2009) focused only on e-commerce and did not include other uses of the Internet, which were addressed in this study.

This dissertation built on previous research by Furnell, Bryant, and Phippen (2007) who recommended further research into promoting cybersecurity awareness among HCUs so that they could develop the necessary skills to protect themselves from the growing threats to their home computers. Furnell et al. (2007) also indicated that many of the attacks on HCUs were motivated by financial gains to the perpetrators, and the success of such attacks were being facilitated by the lack of cybersecurity awareness that existed among HCUs. D'Arcy et al. (2009) also found that cybersecurity awareness was essential in training and developing the cybersecurity skills of Internet users. Such

skills would reduce the cybersecurity vulnerabilities that users face when they use the Internet. Therefore, in response to the call for further research by Furnell et al. (2007), as well as the findings of D'Arcy et al. (2009), Kritzinger and von Solms (2010) developed an enforcement-awareness model which proposed a way to 'force' HCU's to be aware of the risks that were involved when they use the Internet. According to Kritzinger and von Solms (2010), this model would empower HCU's by giving them a better understanding of cybersecurity issues, possible threats, how to avoid the threats, and ultimately, improve their cybersecurity skills. Kritzinger and von Solms (2010) also argued that one of the most important factors that contributed to the vulnerability of HCU's to cyber-attacks was that many of them had limited awareness of cybersecurity countermeasures, and often use the Internet without any cybersecurity awareness or skills. Further, they found that although there were many research projects that identified limited awareness of cybersecurity countermeasures as a problem among HCU's, there was little amount of research done on designing and implementing appropriate cybersecurity awareness programs to solve this problem.

This study had six specific goals. The first specific goal of this research was to empirically assess the contribution of SCCA, CSE, PRIT, and OACTA on their motivation (IM & EM) to acquire cybersecurity skills before (t_1) the cybersecurity awareness training. The second specific goal of this research was to empirically assess the contribution of senior citizens' motivation (IM & EM) to acquire cybersecurity skills on their CyberSkills level before (t_1) the cybersecurity awareness training. These two initial assessments were used as a benchmark point of comparison for the effects of the training. The cybersecurity awareness training was done after the initial

assessment of the aforementioned constructs (t_2). The third specific goal of this research was to empirically assess the contribution of SCCA, CSE, PRIT, and OACTA on their motivation (IM & EM) to acquire cybersecurity skills after (t_3) the cybersecurity awareness training. The fourth specific goal of this research was to empirically assess the contribution of senior citizens' motivation (IM & EM) to acquire cybersecurity skills on their CyberSkills level after (t_3) the cybersecurity awareness training. These two second assessments were done to compare with the pre-training measures and to allow the comparisons of pre-post training levels of the aforementioned constructs. The fifth specific goal of this research study was to empirically assess the difference in the levels of senior citizens' CyberSkills level before (t_1) and after (t_3) the cybersecurity awareness training. This was done to determine if the training had an impact on the aforementioned measurement, that is, to determine if the training had any impact on mitigating the cybersecurity risks. The sixth specific goal of this research was to empirically assess the difference in the levels of senior citizens' CyberSkills level before (t_1) and after (t_3) the cybersecurity awareness training, when controlled for the following eight demographic indicators: (a) age, (b) gender, (c) years of using computers, (d) years of using the Internet, (e) years of using Internet-enabled mobile devices, (f) years of working in corporate or formal organization, (g) years since retiring, and (h) level of education. This was done to determine if there were any indirect effects of the independent variables (IVs) on the dependent variable (DV), through the demographic indicators. Therefore, a better understanding of the relationship, if any, between the demographic indicators and the aforementioned measurements, before and after the training, was provided. In other words, this goal provided stronger indications of the

effects of the IVs on the DV to determine if the relationships between the IVs and DV were the same, or different, when there is control for the demographic indicators.

Research Questions and Propositions

The main research question that this study addressed was: what is the contribution of SCCA, CSE, PRIT, and OACTA on their motivation (IM & EM) to acquire cybersecurity skills, as well as their CyberSkills level, while comparing it before and after cybersecurity awareness training? The six specific research questions were:

RQ1: What is the contribution of SCCA, CSE, PRIT, and OACTA on their motivation (IM & EM) to acquire cybersecurity skills before (t_1) the cybersecurity awareness training?

RQ2: What is the contribution of senior citizens' motivation (IM & EM) to acquire cybersecurity skills on their CyberSkills level, before (t_1) the cybersecurity awareness training?

RQ3: What is the contribution of senior citizens' SCCA, CSE, PRIT, and OACTA on their motivation (IM & EM) to acquire cybersecurity skills after (t_3) the cybersecurity awareness training?

RQ4: What is the contribution of senior citizens' motivation (IM & EM) to acquire cybersecurity skills on their CyberSkills level after (t_3) the cybersecurity awareness training?

RQ5: Are there significant mean difference in the levels of senior citizens' CyberSkills level, before (t_1) and after (t_3) the cybersecurity awareness training?

RQ6: Are there significant mean difference in the levels of senior citizens'

CyberSkills level before (t_1) and after (t_3) the cybersecurity awareness training, when controlled for the following eight demographic indicators: (a) age, (b) gender, (c) years of using computers, (d) years of using the Internet, (e) years of using Internet-enabled mobile devices, (f) years of working in corporate or formal organization, (g) years since retiring, and (h) level of education?

The research model is shown in Figure 1. There were four IVs, namely, SCCA, CSE, PRIT, and OACTA. The mediating variable (MV) was motivation (IM & EM) to acquire cybersecurity skills. Motivation was based on two parts, intrinsic and extrinsic motivation: each was measured separately. The DV was CyberSkills, while the treatment (intervention) was cybersecurity awareness training. The propositions were:

P1_(a & b): There will be a significant positive contribution of SCCA on their (a) IM and (b) EM to acquire cybersecurity skills.

P2_(a & b): There will be a significant positive contribution of senior citizens' CSE on their (a) IM and (b) EM to acquire cybersecurity skills.

P3_(a & b): There will be a significant positive contribution of senior citizens' PRIT on their (a) IM and (b) EM to acquire cybersecurity skills.

P4_(a & b): There will be a significant positive contribution of senior citizens' OACTA on their (a) IM and (b) EM to acquire cybersecurity skills.

P5_(a & b): There will be a significant positive contribution of senior citizens' (a) IM and (b) EM to acquire cybersecurity skills on their CyberSkills level.

P6_(a & b): There will be significant mean difference in the levels of senior citizens' CyberSkills level before (t_1) and after (t_3) the cybersecurity awareness training.

P7_(a to h): There will be significant mean difference in the levels of senior citizens' CyberSkills level before (t_1) and after (t_3) the cybersecurity awareness training, when controlled for the following eight demographic indicators: (a) age, (b) gender, (c) years of using computers, (d) years of using the Internet, (e) years of using Internet-enabled mobile devices, (f) years of working in corporate or formal organization, (g) years since retiring, and (h) level of education.

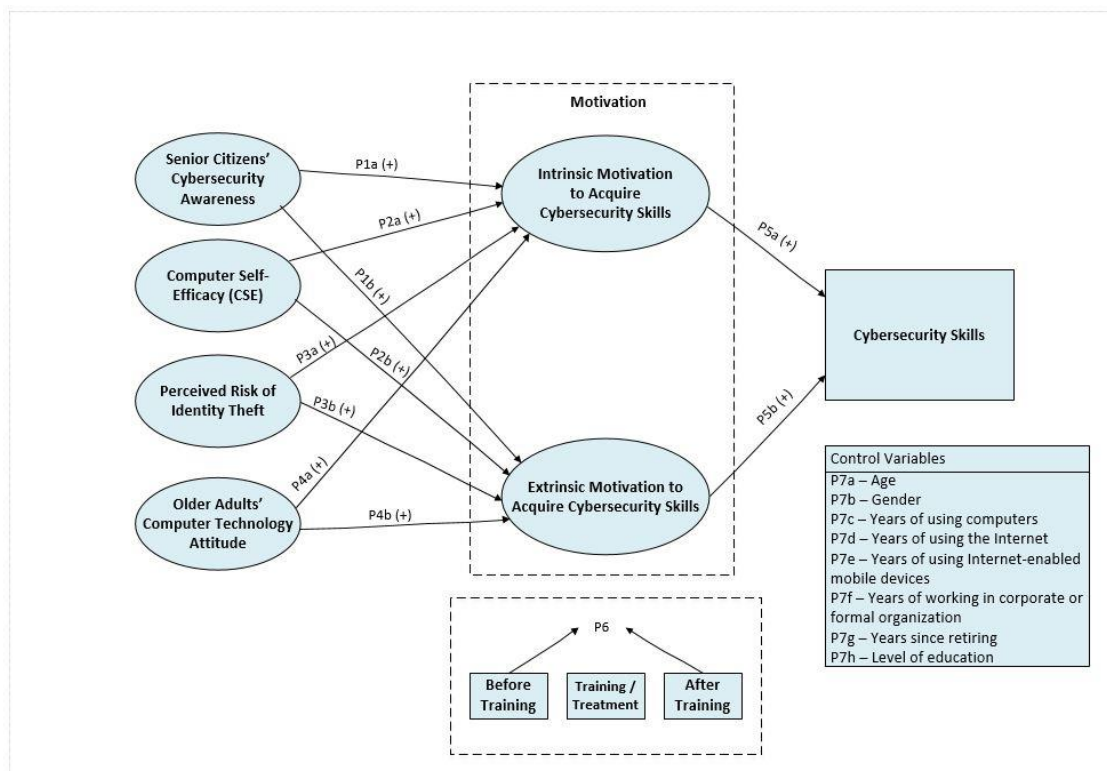


Figure 1. Research Model for Factors that Contribute to Senior Citizen's Motivation to Acquire Cybersecurity Skills

Relevance and Significance

Relevance

This study is relevant as it provides a better understanding of what motivates Internet users, specifically senior citizens, to acquire cybersecurity skills so that they will be empowered to mitigate the effects of cyber-attacks when the attacks occur. As pointed out by Abawajy (2014) and Shillair et al. (2015), cyber-attacks constantly evolve, therefore, it is important to know what motivates Internet users, especially senior citizens, to expend the effort that is necessary, such as acquire cybersecurity skills, to be able to counter these evolving cyber-attacks. Furthermore, the relevance of this study is justified by the phenomenal growth in Internet use amongst senior citizens, coupled with the fact that one in five senior citizens is being targeted and exploited online because they have limited awareness of cybersecurity countermeasures (Claar & Johnson, 2012; Grimes et al., 2010; Perrin & Duggan, 2015; Willis, 2015). Lam and Lee (2006) indicated that senior citizens should be given special consideration for training because they face challenges that were distinct from other groups of Internet users, e.g. short memory span and slow information processing speeds. Additionally, Grimes et al. (2010) highlighted the importance of assessing whether senior citizens who use the Internet were aware of cyber-attacks, and to what extent their limited awareness would place them at greater risk of cyber-attacks. Carlton and Levy (2015) as well as Shillair et al. (2015) also called for specific cybersecurity awareness training for Internet users to counter cyber-attacks, as a large percentage of Internet users was still very naïve about cybersecurity, and hence, fall

prey to these attacks. One of the results from cyber-attacks on the vulnerable group of senior citizens is losses in excess of \$2.6 billion dollars annually (Willis, 2015).

Significance

This study is significant for a number of reasons. Firstly, using Deci and Ryan's (1985) Self-Determination Theory (SDT) to explain human motivation as the theoretical lens, it adds to the body of knowledge on the factors that motivate senior citizens to acquire cybersecurity skills, and thus, reduce the billions of dollars in losses accrued to them because of cyber-attacks (Abawajy, 2014). Wall, Palvia, and Lowry (2013) stated that using SDT to study information security (InfoSec) behavior could make significant theoretical contributions to InfoSec research. Secondly, senior citizens benefitted in that, as a result of the cybersecurity awareness training, they are now better able to identify and mitigate the effects of cyber-attacks, which has had devastating effects on their lives (Jones, 2001). Thirdly, recommendations from this study are useful to law enforcement in reducing the number of reported cases relating to cybersecurity issues amongst senior citizens. Consequently, more law enforcement resources can be freed up to fight other sources of cybercrime such as those that result from organized cyber-criminal groups, for example, online child exploitation and cyberterrorism, which pose serious challenges to the peace and stability of individuals in the society (Akopyan & Yelyakov, 2009; Choo & Smith, 2008).

Barriers and Issues

There were several barriers that this research study faced. Firstly, since this study involved human subjects, permission was needed from the Institutional Review Board

(IRB) before the study could be conducted. Therefore, in order to mitigate any effects that this barrier had on this study, permission was sought from the IRB before the study was conducted.

Secondly, using the Delphi technique is a potential barrier as, care must be given to participant selection, it requires a lot of attention to follow the process, and the questions must be meticulously prepared to avoid ambiguity. Additionally, it may be a challenge to collect enough responses from the expert participants. To mitigate this barrier, a large number of participants was selected to participate in the process.

Thirdly, since the unit of analysis was senior citizens, and there was pre-testing, training, and post-testing, some participants may drop out over the period of the study due to health problems, fatigue or lack of interest. To mitigate these barriers, the following were done: the study period was short, that is, two to three weeks, a large number of senior citizens was recruited, so that even though some dropped out, the remaining number was still a good sample size, plus the testing and training sessions were conducted in small groups.

Limitations and Delimitations

Limitations

Uncontrollable threats to the internal validity of a study are referred to as limitations and it is very important that the limitations be clearly stated so that other researchers can replicate or expand on the study (Creswell, 2005, Ellis & Levy, 2009). Another benefit of stating study limitations is that other researchers can “judge to what extent the findings can or cannot be generalized to other people and situations” (Creswell,

2005, p. 198). Two probable limitations of this study were the use of an expert panel to validate the survey instrument, and the use of volunteers to participate in the pilot test. According to Ellis and Levy (2010), the opinions of experts on an expert panel are limited only to the experts who were recruited to participate, and may not be the best set of opinions. Additionally, the pilot study participants were volunteers and since they can withdraw from the study at any time, the truthfulness of the pilot test results may be questionable (Ellis & Levy, 2010). Such limitations can be mitigated by following the “accepted processes and use established tools as they were designed to be used” (Ellis & Levy, 2010, p. 115). For example, Delbecq, Ven, and Gustafson (1975) recommended the use of a consensus-building process such as the Delphi Technique when expert panels are used. This study combined the Delphi Technique, literature review, and a pilot test to mitigate these limitations. Also, to mitigate the limitation of bias, care was taken to select experts from various industries in varying roles.

Delimitations

Delimitations refer to the scope of the study, will impact the external validity or how generalizable the results of the study will be, and if they are not stated, it will be difficult for readers to understand the boundaries of the study (Ellis & Levy, 2009; Leedy & Ormrod, 2005). This study investigated the factors that would contribute to the motivation of senior citizens to acquire cybersecurity skills so that they will be able to identify as well as mitigate against cyber-attacks. After an extensive review of the literature, the factors that were investigated in this study were SCCA, CSE, PRIT, OACTA, and motivation (IM & EM). Additionally, the participants had to be 60 years or older, and have been accessing the Internet via an Internet-enabled mobile device

(smartphone, tablet/iPad, laptop, etc.) for at least one year. These were delimitations as other factors such as computer anxiety, depression levels, self-esteem, and cognitive decay may also play contributing roles.

Definition of Terms

Research in cybersecurity is expanding and as such there are times when ambiguity exists in terminologies that are used. The following definitions are intended to remove ambiguities that may exist with terms that were used in this study.

Attack Vector – The path that a cyber-criminal uses to gain access to a network server or a computer in order to commit malicious actions (Lemoudden et al., 2013).

Attitude - “refers to one’s positive or negative judgment about a concrete subject” (Abedalaziz et al., 2013, p. 201).

Cognitive Evaluation Theory (CET) – This is one of the sub-theories of self-determination theory and it addressed the factors that would propel human behavioral motivation as well as the situations that would undermine or prompt intrinsic motivation (Deci & Ryan, 1985).

Computer Self-Efficacy - “An individual’s perceptions of his or her ability to use computers in the accomplishment of a task” (Compeau & Higgins, 1995, p. 191).

Cyberspace - “A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (NIST, 2011, p. B-3).

Cybersecurity - “The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation” (NICCS, 2015, para. 2).

Cybersecurity Awareness – “Alerting Internet users of cybersecurity issues and threats, and enhancing Internet users’ understanding of cyber threats so they can be fully committed to embracing security during Internet use” (Rahim et al., 2015, p. 607).

Cybersecurity Skills – “Correspond to an individual’s technical knowledge, ability, and experience surrounding the hardware and software required to execute information security in protecting their IT against damage, unauthorized use, modification, and/or exploitation” (Carlton & Levy, 2015, p. 3).

Financial risk - Refers to any financial or monetary damage or loss that may be incurred from acquiring a product (Featherman & Pavlou, 2003).

Identity Theft - A crime that occurs when a person unlawfully uses another person’s PII for personal gain, for example, to obtain financial benefits, or, with the intention to commit fraud or other crimes (Bellah, 2001; Lai et al., 2012)

Intrinsic Motivation - Occurs when a person performs an activity simply for the fun of it, that is, the person finds the activity satisfying, and does it because of having an interest in the action, rather than by external reinforcement (Deci, 1971).

Extrinsic Motivation - Occurs when a person is moved to do an activity by factors that exist outside of the person, or when the activity is done in response to some external stimuli, for example, to get a reward or benefit (Deci, 1971).

Organismic Integration Theory (OIT) - This is one of the sub-theories of self-determination theory and it addressed different types of extrinsic motivation plus the circumstances that would either promote or deter extrinsic motivation (Deci & Ryan, 1985).

Perceived Risk - “A person’s belief in the likelihood that they will be harmed as a consequence of taking a particular action” (Nemati & Van Dyke, 2009, p. 52).

Performance Risk - Refers to the efficiency of a product or the probability that it may malfunction and might not perform as expected (Featherman & Pavlou, 2003).

Phishing – “Online scams that frequently use unsolicited messages purporting to originate from legitimate organizations, particularly banking and finance services, to deceive victims into disclosing their financial and/or personal identity information (PII) to commit or facilitate other crimes (e.g. fraud, identity theft and theft of sensitive information)” (Choo, 2011, p. 724).

Physical Risk - “Involves the potential threat to an individual’s safety, physical health and wellbeing” (Lu et al., 2005, p. 109).

Privacy Risk - Refers to the “potential loss of control over personal information, such as when information about you is used without your knowledge or permission” (Featherman & Pavlou, 2003, p. 455).

Psychological Risk - Refers to a user’s perception of the potential loss of self-esteem, peace of mind, mental stress, or self-perception/ego that results from worrying or feeling frustrated when a product is used (Featherman & Pavlou, 2003; Liao et al., 2010).

Risk – “A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would

arise if the circumstance or event occurs; and (ii) the likelihood of occurrence” (NIST, 2011, p. B-8).

Security Risk - Refers to concerns that users have regarding potential cyber-attacks on the networks and data transactions during the sending/receiving of financial information online, including but not limited to, network hacks as well as unauthorized access to their financial accounts via false identification (Hanafizadeh & Khedmatgozar, 2012).

Self-Determination Theory (SDT) – This theory differentiates between two types or sources of motivation, namely intrinsic and extrinsic, as well as has been used to explain the human internal propensity to learn through intrinsic motivation (Deci & Ryan, 1985).

Social Risk - Refers to the potential loss of a person’s standing within a social group as a result of using a product, i.e. the probability that the person will perceive that he/she will look foolish to other people that he/she considers to be important (Featherman & Pavlou, 2003; Lu et al., 2005).

Time Risk - Refers to the “potential losses to convenience, time and effort caused by wasting time researching, purchasing, setting up, switching to and learning how to use the e-service” (Featherman & Wells, 2010, p. 114).

Summary

Chapter one provides the background, problem statement, goals, and research questions with corresponding propositions for the research problem under study. It also outlines the relevance, significance, barriers, issues, limitations, delimitations, and definitions of terms. The problem that is being addressed is the increase in the success of cyber-attack vectors due to limited cybersecurity awareness and skills among Internet

users, especially senior citizens, which ultimately causes them significant financial losses (Abbasi et al., 2010; D'Arcy et al., 2009; Purkait et al., 2014). The problem was addressed by empirically assessing the factors that would motivate senior citizens to acquire cybersecurity skills so that they can identify, as well as know how to mitigate against cyber-attacks, and thus reduce the billions of dollars in losses accrued to them because of cyber-attacks. As stated in the main goal, this study empirically assessed the contributions of SCCA, CSE, PRIT, and OACTA on their motivation (IM & EM) to acquire cybersecurity skills, as well as their CyberSkills level, while comparing each before and after cybersecurity awareness training. This study expanded the literature on the dangers and consequences of having limited cybersecurity awareness and skills as well as how to motivate users to heed the warnings to acquire the skills necessary for cyber-attack mitigation (Abawajy, 2014; Carlton & Levy, 2015; Grimes et al., 2010; Ramim & Levy, 2006; Shillair et al., 2015). It also built on the work of prior researchers who had recommended increasing cybersecurity awareness and skills among Internet users, for example, senior citizens, as a means of reducing the effects of cyber-attacks (Choo, 2011; D'Arcy et al., 2009; Furnell et al., 2007; Kritzinger & von Solms, 2010; Rahim et al., 2015). This study is relevant and significant for the following reasons: it adds to the body of knowledge on the factors that would motivate senior citizens to acquire cybersecurity skills as a countermeasure to cyber-attacks (Abawajy, 2014); through the training session, senior citizens were better able to identify and mitigate the effects of cyber-attacks which has had devastating effects on their lives (Jones, 2001); and the study's recommendations can be useful to law enforcement in reducing the

number of reported cases relating to cybersecurity issues amongst senior citizens
(Akopyan & Yelyakov, 2009; Choo & Smith, 2008).

Chapter 2

Literature Review

Introduction

According to Hart (1998), a literature review is “the use of ideas in the literature to justify the particular approach to the topic, the selection of methods, and demonstration that this research contributes something new” (p. 1). Further, for the literature review to be effective, it should create “a firm foundation for advancing knowledge. It facilitates theory development, closes areas where a plethora of research exists, and uncovers areas where research is needed” (Webster & Watson, 2002, p. 13). As recommended by Levy and Ellis (2009), this IS-related literature review was done utilizing sources that contained “IS research publications (i.e. journals, quality conference, proceedings, etc.) that are valid to the proposed study” (p. 183). The information contained herein was drawn from several disciplines, including but not limited to IS, criminology, and gerontology. Consequently, the literature review presented in this chapter laid the theoretical foundation as well as provided a synopsis of information pertaining to all the IVs, DV, and other variables used in this study.

Theoretical Foundation - Motivation

Different perspectives of motivation have been used to study human behavior in an effort to understand how an individual behaves (Liaw, 2002). As such, there is an extensive body of literature that describes different motivation theories. For clarification purposes, Maslow (1943) pointed out that theories about motivation were not the same as

theories related to behavior, rather, “the motivations are only one class of determinants of behavior. While behavior is almost always motivated, it is also almost always biologically, culturally and situationally determined as well” (p. 371). Ryan and Deci (2000) stated that “to be motivated means *to be moved* to do something. A person who feels no impetus or inspiration to act is thus characterized as unmotivated, whereas someone who is energized or activated toward an end is considered motivated” (p. 54). Thus, motivation “refers to an individual’s drive to accomplish particular tasks and propels the individual along a certain trajectory. Motivation also determines the level of intensity and persistence a person might use to complete tasks” (Hall & Marshall, 2016, p. 293). Further, motivation will determine and guide how a person behaves when performing an activity (Cota, Ishitani, & Vieira, 2015).

Deci and Ryan (1985) presented SDT as a theory of human motivation that focused on the factors that would initiate an individual’s behavior. SDT, therefore, provided a broad theoretical framework to study human motivation and has also been used as an explanation for human internal propensity to learn through intrinsic motivation (Chris Zhao & Zhu, 2014, Deci & Ryan, 1985; Ryan & Deci, 2000). Based on the different reasons or goals that causes a person to act, SDT differentiated between the different types or sources of motivation and classified them as intrinsic or extrinsic (Deci, 1971; Ryan & Deci, 2000). If a person performs an activity simply for the fun of it with no apparent reward, the person is intrinsically motivated, however, if the person performs the activity because of an apparent reward, the person is extrinsically motivated (Deci, 1971). Hence, SDT helps to differentiate between behaviors that originate from an individual’s sense of self, and behaviors that do not, that is, behaviors that were

volitional, plus accompanied by the experience of freedom and autonomy, versus behaviors that were accompanied by the experience of pressure and control (Ryan & Deci, 2000). SDT is a meta-theory that includes sub-theories, two of the main ones are cognitive evaluation theory (CET) and organismic integration theory (OIT) (Chris Zhao & Zhu, 2014; Deci & Ryan, 1985). CET addressed the factors that drove human behavioral motivation along with the situations that would undermine or prompt intrinsic motivation, whereas OIT addressed different types of extrinsic motivation along with the situations that would promote or deter extrinsic motivation (Deci & Ryan, 1985; Lee et al., 2015). Lee et al. (2015) indicated that three facilitators of human motivation were proposed in CET, namely autonomy, relatedness, and competence. Autonomy referred to an individual's desire to participate in activities that he/she chooses, that is, to direct his/her own course of action; relatedness referred to an individual's feelings of connectedness; and, competence referred to an individual's desire to effectively interact with the environment so that the individual could control the outcomes of his/her own actions, that is, to produce desirable outcomes and prevent undesirable outcomes (Lee et al., 2015; Wall et al., 2013). CET posits that intrinsic motivation can be facilitated by supporting the individual's needs for autonomy and competence, whereas, thwarting those needs can forestall intrinsic motivation (Ryan & Deci, 2000). In the OIT sub-category of SDT, the different forms of extrinsic motivation, along with the contextual elements that either promote or deter internalization and integration of the regulation for behaviors was outlined (Deci & Ryan, 1985). The different forms of extrinsic motivation were differentiated by the degree of autonomy expressed by an individual (Deci & Ryan, 1985). Inherent in OIT was the proposition that extrinsic motivation could vary in its

relative autonomy, hence OIT offered a path from being entirely extrinsically motivated to a form of motivation that shared most of the experiential aspects that were common in intrinsic motivation (Deci & Ryan, 1985; Lee et al., 2015; Ryan & Deci, 2000). Thus, as an individual internalized external regulation into their sense of self, the more the individual would feel and behave as though he/she was intrinsically motivated (Deci & Ryan, 1985; Rigby, Deci, Patrick, & Ryan, 1992).

With its origin in the psychology domain, motivation has been widely used in various other domains to explain how humans behave or act (Lee et al., 2015). For example, in education, Lin, McKeachie, and Kim (2002) studied intrinsic motivation (preference for challenge), and extrinsic motivation (to get good grades) of college students in traditional course structures. Lin et al. (2002) reported that intrinsically motivated students persisted longer in a course and achieved higher grades than those who were extrinsically motivated. However, to best achieve persistence in learning, a moderate level of extrinsic motivation coupled with a high level of intrinsic motivation was recommended (Lin et al., 2002). Teo et al. (1999) had also indicated that motivation theorists had posited that both intrinsic and extrinsic motivation determine a person's performance or actions. Within the InfoSec domain, motivation is relevant as it can provide important perspectives on the actions of computer users, and, thus, offer explanations on the factors that motivate the users to behave the way they do towards information systems (IS) (Lee et al., 2015). Although SDT has been found to contribute to positive behavioral outcomes, and increased intrinsic motivation, psychological well-being, persistence as well as initiative, it has not been widely used in InfoSec research (Wall et al., 2013). Additionally, Wall et al. (2013) stated that SDT can be a useful lens to

study InfoSec behavior that were intrinsically motivated and that SDT could make an important theoretical contribution to InfoSec research. Therefore, this study used motivation, specifically, the intrinsic and extrinsic motivation of SDT, as the theoretical foundation to investigate the factors that will motivate senior citizens to acquire cybersecurity skills so that they will be able to identify and mitigate cyber-attacks. The factors that were investigated were SCCA, CSE, PRIT, and OACTA.

There are reports in the literature that indicate that there is a relationship between motivation and cybersecurity awareness (Claar & Johnson, 2012; McCrohan, Engel, & Harvey, 2010). Claar and Johnson (2012) as well as McCrohan et al. (2010) found that cybersecurity awareness improved the cautious actions of Internet users, positively influenced their ability to detect cyber-attacks, and motivated secure Internet use amongst them. Additionally, increased cybersecurity awareness improved the Internet users' self-efficacy, and hence motivated them to take mitigating actions towards cyber-attacks (Albrechtsen & Hovden, 2010; White, 2015; Wolf, Haworth, & Pietron, 2011). However, Wolf et al. (2011) also found that the effectiveness of cybersecurity awareness diminished over time, and suggested that other factors that can sustain motivation after cybersecurity awareness training, should be investigated.

Boss, Kirsch, Angermeier, Shingler, and Boss (2009) investigated factors that could motivate computer users to follow IS security policies. Lack of motivation (apathy) and computer self-efficacy (CSE) were found to be important variables that influenced users' decisions related to IS security behaviors: users had to be motivated before they would perform IS security activities, as well as felt confident in their abilities to use the computer to perform the required activities (Boss et al., 2009). Thus, Boss et al. (2009)

recommended that future research should investigate the theoretical relationships between motivation and CSE with IS security. Similarly, Rhee, Kim, and Ryu (2009) investigated self-efficacy in the InfoSec (SEIS) context to see how it would influence the security actions and motivation of Internet users to strengthen their security efforts. Rhee et al. (2009) found, among other things, that SEIS influenced the decision of users to continue as well as strengthen their security efforts. Rhee et al. (2009) also called for further investigation into how CSE would influence and motivate the development of SEIS.

Regarding the relationship between perceived risk and motivation, there are contradictory findings. For example, Yazdipour and Neace (2013) posited that the uncertainty that comes with the perception of risk should produce psychological discomfort, which should ultimately motivate users to take mitigating actions to reduce the discomfort. However, Workman, Bommer, and Straub (2008) noted that users would not always take known mitigating actions against risks because the level of the user's perceived risk would influence how motivated the user would be to take the required mitigating actions. Further, Liang and Xue (2010) found a negative interaction between the levels of a user's perceived risk and the user's motivation to take mitigating actions. On the other hand, Johnston and Warkentin (2010) suggested that when users were made aware of risks regarding cybersecurity threats, the users would be more motivated to take mitigating actions. For example, users were motivated to use protective software when there were perceptions of threats (Johnston & Warkentin, 2010). These contradictory findings indicate that further research regarding perceived risk and motivation is warranted.

Within the context of technology usage, Teo et al. (1999) investigated the role of motivation in the continued usage of the Internet. It was found that although both intrinsic and extrinsic motivation played positive roles in participants' Internet usage, extrinsic motivation played the stronger role (Teo et al., 1999). Therefore, Teo et al. (1999) recommended that further research should be conducted to investigate the role of both intrinsic and extrinsic motivation in the continued use of information technologies. Liaw (2002) also reported that motivation was a key determinant in attitude towards the use of information technologies. Specifically, the computer and Internet experience, motivation, as well as self-efficacy of individuals were key elements towards the attitudes that the individuals have towards the use of the Web (Liaw, 2002).

Research has also shown that there is a positive relationship between Internet users' motivation to take active roles towards mitigating cyber-attacks and their cybersecurity skills level (Holt & Turner, 2012; Inan, Namin, Pogrund, & Jones, 2016, Mohamed & Ahmad, 2012). When Internet users were confident that they possessed cybersecurity skills, they were motivated to play active roles to protect themselves and their PII in the event of cybersecurity threats (Mohamed & Ahmad, 2012). Since acquiring skills such as cybersecurity skills is new for senior citizens, there has been call for more research into investigating other factors, specifically extrinsic motivators that would motivate senior citizens to acquire new skills (Phipps, Prieto, & Ndinguri, 2013). This call was made after it was concluded that intrinsic motivators may be insufficient to increase the motivation to acquire new skills in senior citizens (Phipps et al., 2013). Additionally, to acquire new skills, adult learners need to be sufficiently motivated, which, should then drive them to invest the requisite time and effort to acquire the skills

(Phipps et al., 2013). Prior research supported similar claims that intrinsic motivation decreased as age increased, however, no significant relationship with extrinsic motivation and age or gender was reported (Lepper, Corpus, & Iyengar, 2005; Ryan & Deci, 2000). Ryan and Deci (2000) further indicated that extrinsic motivational factors must be present in order to have persistence in an activity. The main goal of this study was to empirically investigate factors such as SCCA, CSE, PRIT, and OACTA to see their contribution to motivation (IM & EM) to acquire cybersecurity skills in senior citizens. The intent was to provide a better understanding on what motivates senior citizens to acquire cybersecurity skills so that they can mitigate the effects of cyber-attacks.

Intrinsic and Extrinsic Motivation

As previously mentioned, intrinsic motivation occurs when a person performs an activity simply for the fun of it, that is, the person finds the activity satisfying, and does it because of having an interest in the action, rather than by external reinforcement (Deci, 1971; Feng, Fu, & Qin, 2016; Lee, Cheung, & Chen, 2005). On the other hand, extrinsic motivation occurs when a person is moved to do an activity by factors that exist outside of the person, or when the activity is done in response to some external stimuli, for example, to get a reward or benefit (Deci, 1971; Feng et al., 2016; Lee, et al., 2005). Intrinsic and extrinsic motivators are, thus, “two different types of drivers capable of evoking specific outcome behaviour” (Lee et al., 2005, p. 1097). Further, according to Ryan and Deci (2000):

Intrinsically motivated behaviors, which are performed out of interest and satisfy the innate psychological needs for competence and autonomy are the prototype of self-determined behavior. Extrinsically motivated behaviors - those that are

executed because they are instrumental to some separable consequence - can vary in the extent to which they represent self-determination. Internalization and integration are the processes through which extrinsically motivated behaviors become more self-determined. (p. 65)

Since intrinsic motivation occurs when a person performs an activity simply for the fun of it, the person would be more willing to devote extra time and effort to the activity being performed (Cota et al., 2015; Hall & Marshall, 2016; Lee et al., 2015). Conversely, if a person is not intrinsically motivated, the person might devote very little time and effort, if any, which may result in failure at the activity due to having little desire to succeed at the activity (Cota et al., 2015; Hall & Marshall, 2016). Ryan and Deci (2000) stated that higher quality learning was related to intrinsic motivation and individuals who were more intrinsically motivated would display longer persistence than those who were only highly extrinsically motivated. Performing cybersecurity countermeasures requires extra effort, therefore, Internet users, especially senior citizens, must be motivated before they can commit to expending the extra effort that is required (Boss et al., 2009; Shillair et al., 2015).

Table 1

Summary of Motivation-related (Intrinsic & Extrinsic) Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Boss et al., 2009	Empirical investigation	1671 users from a large medical center in southeastern US	Survey: Specification, evaluation, rewards, and precaution. Control	Perception of mandatoriness had a significant positive impact on motivating individuals to take security

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			variables: CSE and apathy	precautions; users had to be motivated before they would engage in IS security activities.
Chris Zhao & Zhu, 2014	Empirical investigation	422 Chinese crowdsourcing contestants	Motivation (external, introjected, identified, integrated, & intrinsic), task granularity, participation effort, and support of motivational affordances (autonomy, competence, relatedness, & leadership)	Regarding participation effort in crowdsourcing contests, the various motivations play different roles. The relationship between motivation and participation effort might be strengthened when there is support for perceived motivational affordances.
Claar & Johnson, 2012	Empirical investigation	184 university undergraduate students	Survey: Health Belief Model (HBM) constructs (perceived vulnerability, perceived severity, perceived benefits, perceived barriers, cues to action, & self-efficacy), prior experience, and computer security usage	Demonstrated that some constructs in the HBM (perceived vulnerability of a security incident & prior experience with a security incident) were more effective than the other constructs in motivating users to use computer security software.
Cota et al., 2015	Developmental	10 adults, age 60 years or more	Games, questionnaires, and interviews: Intrinsic and extrinsic motivation	Developed a digital catalog of games which identified senior citizens preferences and motivation

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				regarding game genres; playing digital games improved the quality of life and mental health of senior citizens.
Deci, 1971	Empirical investigation	Experiment 1: 24 students; Experiment 2: 6 participants Experiment 3: 24 students	Laboratory experiments and observation: Extrinsic motivation (rewards) and intrinsic motivation	Using money as a reward negatively impacted intrinsic motivation; verbal reinforcement and positive feedback positively impacted intrinsic motivation.
Deci & Ryan, 1985	Theoretical review	Classical definitions	SDT	Presented SDT that can be used to provide a theoretical framework to study human motivation. SDT differentiated between intrinsic and extrinsic motivation.
Feng et al., 2016	Empirical investigation	218 mobile phone users	Questionnaire: Timeliness, localization, consumer innovativeness, personalization, perceived enjoyment, attitude, intrinsic and extrinsic motivation	Intrinsic and extrinsic motivation mediated the impacts of the advertising messages on the attitudes of mobile phone users toward mobile advertising; timeliness, localization, and personalizing the advertisement message were antecedents of extrinsic motivation;

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				consumer innovativeness and perceived enjoyment were antecedents of intrinsic motivation.
Hall & Marshall, 2016	Discussion		Intrinsic and extrinsic motivation	Motivation should be fostered in both gifted and mixed abilities classroom settings; gamification in education positively impacts learning outcomes.
Johnston & Warkentin, 2010	Experiment and model development	311 university faculty, staff, and students	Survey: Behavioral intent, social influence, response efficacy, self-efficacy, threat severity, and threat susceptibility	Threat perception is a central component of users' motivation to use protective software; although not uniform across all users, fear appeals impact the behavioral intentions of users to comply with recommended individual acts of security.
Lee et al., 2005	Empirical investigation	544 university students	Questionnaire: Intrinsic motivation (perceived enjoyment), extrinsic motivation (perceived ease of use & perceived usefulness), attitude and behavioral intention	Both intrinsic and extrinsic motivation significantly impacted students' intention to use an Internet-based learning medium.
Lepper et al., 2005	Empirical investigation	797 public school students	Survey: Motivation	Only a moderate correlation existed

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			(intrinsic & extrinsic), social desirability, and academic achievement	between intrinsic and extrinsic motivation; students in lower grades had higher levels of intrinsic motivation than those in higher grades; extrinsic motivation was negatively correlated with academic outcome.
Liang & Xue, 2010	Empirical investigation	152 university business students	Survey: Perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, avoidance motivation, and avoidance behavior	IT threat avoidance behavior of users was predicted by avoidance motivation, which, was consequently determined by self-efficacy, perceived threat, safeguard effectiveness, and safeguard cost. In threat situations, users were more motivated to avoid the threat based on safeguard effectiveness, safeguard cost, and self-efficacy.
Liaw, 2002	Empirical investigation	260 university students	Questionnaire: Computer experience, Web attitude (self-efficacy, enjoyment, usefulness, and intention to use)	Motivation played a very important role in attitude towards the use of information technologies. Key factors identified for attitudes towards using the Web were computer and Internet experience, motivation, and

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				self-efficacy of individuals.
Lin et al., 2002	Empirical investigation	650 college students	Survey: Intrinsic and extrinsic motivation	Positive relationship observed between grades and intrinsic motivation; best combination is a moderate level of extrinsic motivation coupled with high intrinsic motivation.
McCrohan et al., 2010	Empirical investigation	396 university undergraduate business students	Questionnaire: Cyber threat education and awareness, user security behavior	Training and awareness programs aimed at exposing users to information security procedures and threats against their e-commerce activities positively influence security behavior.
Phipps et al., 2013	Model development		Age, ability, perceived self-efficacy, learning intention, and learning	Important to integrate motivational strategies into the learning process for older adults to achieve best learning results; perceived self-efficacy, age, ability, and learning intentions were central to successful learning in older adults.
Ryan & Deci, 2000	Theoretical review	Classical definitions	SDT, intrinsic and extrinsic motivation	Human's natural propensity to learn and assimilate was reflected through intrinsic motivation. Extrinsic

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				motivation can either reflect external control or true self-regulation.
Shillair et al., 2015	Empirical investigation	161 adult home Internet users	Survey: Personal responsibility, intention to engage in online safety behavior, response efficacy, coping self-efficacy, and technology awareness	Combining self-efficacy and personal responsibility interventions can positively impact motivation to engage in online safety behavior.
Teo et al., 1999	Empirical investigation	1370 participants	Questionnaire: Intrinsic motivation, extrinsic motivation, and Internet usage	Both intrinsic and extrinsic motivation played positive roles in participants' Internet usage, however, extrinsic motivation played the stronger role.
Wall et al., 2013	Empirical investigation	94 government employees	Online survey: Self-determination, psychological reactance, self-efficacy, response efficacy, and compliance intention	Recommended that SDT be used in InfoSec research to provide insights into security behaviors that are intrinsically motivated and internalized. Autonomy and efficacy are important control-related motivations in InfoSec.
Workman et al., 2008	Empirical investigation	588 employees from a large corporation that offers technology-	Online questionnaire and direct observations of behavior: Perceived	The level of motivation to prevent a threat from happening was determined by the extent to which

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
		oriented services	severity, vulnerability, locus of control, self-efficacy, response efficacy, response cost, subjective omissive behavior, and objective omissive behavior	the severity of the threat was perceived.

Cybersecurity

Definition and Importance

The National Initiative for Cybersecurity Careers and Studies [NICCS] (2015) defined cybersecurity as “the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation” (para. 2). Major tenets of cybersecurity include understanding the issues of cyber-attacks as well as formulating countermeasures that will preserve the confidentiality, integrity, and availability of information technologies (Jang-Jaccard & Nepal, 2014). von Solms and van Niekerk (2013) extended the definition of cybersecurity to highlight the difference between cybersecurity and InfoSec, two terms that have been frequently used interchangeably. According to von Solms and van Niekerk (2013), “cybersecurity goes beyond the boundaries of traditional information security to include

not only the protection of information resources, but also that of other assets, including the person him/herself” (p. 97). Cybersecurity, along with its challenges, is, therefore, not specific to any one discipline, but rather has a multidimensional interdisciplinary nature that spans various industries, various countries, and individuals (Craigen, Diakun-Thibault, & Purse, 2014). Further, effectively addressing cybersecurity issues involves recognizing that although the issues may be inherent in technologies, the creation of policies governing the use of the technologies, which may include political agreements that cross national borders, is equally important (Mulligan & Schneider, 2011).

Especially with the ubiquitous use of the Internet, cybersecurity is now very relevant, and has global recognition, with over 50 countries publishing national strategy documents on how to handle cybersecurity issues against their critical infrastructures, economies, and their citizens (Okuku, Renaud, & Valeriano, 2015; von Solms & van Niekerk, 2013).

Critical infrastructure systems such as airports, a nation’s oil pipelines, water, and power grids are the life-line of society, therefore, the security and reliability of these systems are of top importance (Jang-Jaccard & Nepal, 2014). Usually, cyber systems are the backbone of these critical infrastructures, hence, a lot of emphasis is placed on limiting cybersecurity vulnerabilities to these systems (Jang-Jaccard & Nepal, 2014). Therefore, cybersecurity is a complex issue, and inadequate cybersecurity has been cited as the biggest threat to success in the information age, as it includes the ability to protect the use of cyberspace from cyber-attacks (Mulligan & Schneider, 2011; National Institute of Standards and Technology [NIST], 2011). According to NIST (2011), cyberspace is “a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet,

telecommunications networks, computer systems, and embedded processors and controllers” (p. B-3). Crimes in cyberspace are escalating as cyberspace offers many advantages to cyber-criminals including but not limited to a greater assurance of anonymity over the use of other paths, such as the telephone, crimes can be done remotely on a wider scale simultaneously, and automation of criminal acts (Brenner, 2006). This global reach of cyberspace adds to the complexity of cybersecurity, and Internet users, especially senior citizens, who venture into cyberspace with limited cybersecurity awareness or skills become more vulnerable to cyber-attacks (Kritzinger & von Solms, 2010; Mulligan & Schneider, 2011).

Table 2

Summary of Cybersecurity-related Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Brenner, 2006	Chapter analysis		Cybercrimes	The combination of advancements in technology with cyberspace adds to the complexity of cybersecurity.
Craigen et al., 2014	Literature review and discussions with cybersecurity experts	Articles from various academic disciplines, plus discussions with cybersecurity practitioners, academics, and graduate students		Provided a new definition of cybersecurity that captured its multidimensionality, was more inclusive, and unifying.
Jang-Jaccard & Nepal, 2014	Review and discussion		Existing vulnerabilities in hardware, software and networks; emerging threats in	Incremental patches to cybersecurity issues are not effective to accommodate future needs. An approach to think “outside

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			social media, cloud computing, smartphones and critical infrastructures	box” is recommended to address these types of issues.
Mulligan & Schneider, 2011	Essay			Provided a rational, defensible, and legitimate doctrine of public cybersecurity.
Okuku et al., 2015	Exploratory study	50 Kenyan ICT stakeholders	Survey	Countries that have vibrant mobile Internet users must play more active roles in improving the cybersecurity awareness of the users, e.g. providing secured and robust technological frameworks as well have more stringent cybercrime laws.
von Solms & van Niekerk, 2013	Exploratory study		Scenarios and examples	Differentiates between the definitions of cybersecurity and information security.

Cybersecurity Threats and Cyber-Attacks

Inan et al. (2016) states that cybersecurity threat refers to:

Any potentially harmful processes and actions performed to (1) access and use private information (e.g., identity theft), (2) attempt to deceive and scam users (e.g., spam emails), (3) install software intended to perform an unauthorized process (e.g., viruses & malware), or (4) directly attack computer systems and networks (e.g., hacking). (p. 29)

A cyber-attack refers to an attack that happens in cyberspace that targets an enterprise's or individual's "use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" (NIST, 2011, p. B-3). Hence, Internet users who lack awareness of cybersecurity threats would be more vulnerable to cyber-attacks (Inan et al., 2016; Kritzinger & von Solms, 2010). Amidst the many benefits of the Internet, comes numerous and new opportunities for cyber-attacks, mainly because the combination of computer technologies with cyberspace has removed geographic boundaries (Brenner, 2006; Choo, 2008; Roberts, Indermaur, & Spiranovic, 2013). For example, the Internet has extended the geographic reach of criminal activities, created new types of criminal activities, and provided new ways to conduct existing crimes, such as identity theft and phishing (Choo, 2008; Roberts et al., 2013; Savona & Mignone, 2004). As such, cyberspace provides a safe haven for the development and enrichment of cyber-attacks, ultimately making them threats to the economic and social stability of society (Choo, 2008). Cyber-attack is one of the prime concerns that threatens society, and the rapid increase in the number of cyber-attack incidents has raised the alarm for the provision of strategies that can protect users in cyberspace (Inan et al., 2016). A Symantec Corporation (2014) report adds support to the claim that there is rapid increase in the number of cyber-attack incidents revealing: a rise in phishing rate with the global average phishing rate increasing from 1 in 414 in 2012 to 1 in 392 in 2013 (February was the busiest month where the rate rose to 1 in 193 emails); over 552 million identities exposed through data breaches; an overall 91% increase in targeted attacks, and 62% increase in the number of breaches in 2013. Similarly, Jang-Jaccard and Nepal

(2014) reported that, in 2012, cyber-attacks cost approximately \$114 billion, while in 2014, McAfee Inc. estimated that more than \$400 billion had accrued to the global economy because of cyber-attacks. Cyber-attacks are flourishing because they are cheaper to commit, convenient and involve less risks than traditional crimes; perpetrators require very little beyond a computer and Internet connection to launch such attacks (Jang-Jaccard & Nepal, 2014). Moreover, not very high levels of technological skills are required to launch such attacks especially since many toolkits are easily available and downloadable over the Internet (Levy, Ramim, & Hackney, 2013). Among the industries, the banking and finance service industries have been singled out as the most targeted industries for cyber-attacks (Choo, 2011). This is because millions of online financial transactions are conducted daily in which users are required to use their PII, and this make them vulnerable to cybercrimes such as identity theft, credit card and bank fraud, as well as other financially-motivated cyber-attacks (Choo, 2011; Davinson & Sillence, 2014). Unsecured Wi-Fi networks and phishing attacks have been identified as the most common cyber-attack vectors used by cyber-criminals to get to the PII of Internet users for malicious purposes (Futcher, 2015; Lemoudden et al., 2013; Noor & Hassan, 2013). Therefore, cybersecurity awareness and skills programs that will alert Internet users to cyber-attacks as well as increase their cybersecurity skills appear to be warranted to counter and reduce the effects of cyber-attacks.

Table 3

Summary of Cybersecurity Threats and Cyber-Attacks Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Brenner, 2006	Chapter analysis			Nations need to unite and agree on methods to assert jurisdiction over transnational cyber-criminals. This is needed to ensure that cyber-criminals do not exploit jurisdictional conflicts for their benefit.
Choo, 2008	Discussion			New response strategies such as strengthening of laws are necessary to counter new cyber-attacks facilitated by new technologies and rapid advancement in ICT.
Choo, 2011	Literature review			More investment in research and development into cybersecurity is needed to counter the fast-moving cyber threat landscape.
Davinson & Sillence, 2014	Empirical investigation	20 participants comprising students, retirees, and currently employed	Semi-structured interviews; HBM components (perceived susceptibility, perception of fraud prevalence, personal susceptibility, perceived severity, perceived cost, perceived benefits,	Users' levels of awareness of cybersecurity threats did not match their levels of knowledge and skills about how to counteract the threats.

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Inan et al., 2016	Empirical investigation	20 visually impaired individuals	cues to action, perceived control, & awareness of behaviors to control fraud) Interviews and questionnaire; technology/Internet use, cybersecurity threats and concerns, and cybersecurity knowledge, attitudes, beliefs, and confidence	High levels of cybersecurity knowledge and skills led to high concerns toward cybersecurity threats, and less use of the Internet.
Levy et al., 2013	Empirical investigation	519 university business students	Survey: Attacks on the server, email interception, unauthorized file sharing, unauthorized access, and spoofing attacks	Most participants thought that cyber-attacks on e-learning systems were unethical or very unethical.
Roberts et al., 2013	Exploratory study	1550 participants	Survey: Fear of cyber-identity theft and related fraudulent activity	Fear of cyber-attacks equates or exceeds fear of traditional place-based crimes. This can restrict the growth and development of e-commerce.
Savona & Mignone, 2004	Analysis			Advancements in ICT have facilitated the increase in cyber-attacks. The scientific research community should provide understanding of this new phenomena.

Cyber-attack Vectors

An attack vector is a path through which a cyber-criminal can gain access to a network server or a computer to deliver a malicious effect or obtain information for malicious purposes (Lemoudden et al., 2013). The widespread use of cyber-attack vectors such as unsecured Wi-Fi networks and phishing attacks by Internet users with limited cybersecurity skills, has contributed to the increase in the success of such cyber-attack vectors (Futcher, 2015; Noor & Hassan, 2013). Wi-Fi networks use broadcast signals to communicate, hence, they are viewed as borderless in nature, and this contributes to their vulnerability to cyber-attacks (Budhrani & Sridaran, 2014; Noor & Hassan, 2013). Therefore, Internet users have been cautioned against using unsecured Wi-Fi networks to access services that are of a sensitive, for example, financial services (Aïmeur & Schonfeld, 2011). Common cyber-attacks on Wi-Fi networks include packet sniffing, social engineering, rogue access points, and man in the middle attacks (Noor & Hassan, 2013). The passive nature of these types of attacks make them even more dangerous to Wi-Fi users who can have their private and confidential information compromised (Noor & Hassan, 2013). Advancements in technology such as the ubiquitous use of mobile Internet-enabled devices (laptops, tablets/iPads, smartphones) coupled with the tethering features of these devices have also contributed to the popularity of hotspots which make it much easier for cyber penetration by cyber-criminals (Budhrani & Sridaran, 2014; Jang-Jaccard & Nepal, 2014; Noor & Hassan, 2013). Hotspots provide free Wi-Fi connections to mobile device users, however, many mobile device users appear to be unaware that not all hotspots are secure, thus, increasing their risks of cyber-attacks via such means (Imgraben, Engelbrecht, & Choo, 2014). Approximately 48% of 250

surveyed participants admitted to leaving their Wi-Fi on at all times on their mobile devices, with some also accessing sensitive financial information while connected to unknown Wi-Fi networks via their mobile devices (Imgraben et al., 2014). Another contributing factor to the success of cyber-attacks via unsecured Wi-Fi networks is the wide availability and easy accessibility of hacking tools which are used by cyber-criminals to attack unsuspecting Internet users on unsecured Wi-Fi networks (Noor & Hassan, 2013). Cyber-criminals can also use the hacking tools to poison the Web browser caches of Wi-Fi network users, and once poisoned, the users' devices can be redirected to phishing sites at a later date, even when the users are connected to other networks (Budhrani & Sridaran, 2014). Cyber-criminals also use phishing attacks to carry out their crimes, and a lack of awareness of these types of attacks amongst Internet users have been blamed for the increase in the success of such attacks (Abbasi et al., 2010; Futcher, 2015; Purkait, 2012). In phishing attacks, the vulnerability of humans is directly targeted, and this is done by enticing them to visit fraudulent websites after circumventing the cybersecurity measures that they have in place on their devices (Choo, 2011; Hong, 2012; Purkait, 2012). Consequently, phishing attacks have become a very common cyber-attack vector through which cyber-criminals can steal the PII of unsuspecting Internet users (Anderson, Durbin, & Salinger, 2008; Choo, 2011; Purkait, 2012). The stolen PII is often used in identity theft, which can result in billions of dollars in losses per year to unaware Internet users (Anderson et al., 2008; Choo, 2011; Purkait, 2012). Paek and Nalla (2015) reported that Internet users who received phishing attempts were more likely to become identity theft victims, and the likelihood of identity theft increased by two percent with each additional phishing attempt. Senior citizens were less likely to be able to identify

phishing attacks than younger people, however, cybersecurity awareness training that includes cybersecurity skills training should mitigate the effects of such attacks (Futcher, 2015; Purkait et al., 2014).

Table 4

Summary of Cyber-Attack Vectors Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Abbasi et al., 2010	Series of comparison experiments	Numerous existing fake website detection systems tested on 900 websites.	Statistical learning theory (SLT)	Used SLT to develop a prototype to detect fake websites which proved to be more accurate than existing systems.
Budhrani & Sridaran, 2014	Analysis			Wi-Fi local area networks are most vulnerable to cyber-attacks and highly prone to threats of hacking.
Choo, 2011	Literature review			Identified emerging cyber-attack vectors. Proposed using criminological theories to reduce the risk of cybercrime.
Futcher, 2015	Developmental	Focus group of eight individuals comprising academic staff and research students	Questionnaire with three feedback questions on the proposed email phishing attack framework	Developed an email phishing attack framework to raise user awareness of phishing attacks; framework has nine sequential steps that users should ask themselves when trying to decide if an email should be trusted or not. The success of phishing attacks can be mitigated through user awareness.

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Imgraben et al., 2014	Empirical investigation	250 smart mobile device owners	Survey: General security (loss/theft), malware, unauthorized access, phishing, and security (Wi-Fi & Bluetooth)	Overall, the value of participants' collective identities to cyber-criminals was underestimated. Participants did not view cybercrime as a real threat, and hence did not recognize the risks involved. To mitigate the effects of such misconceptions, training was recommended.
Noor & Hassan, 2013	Literature review			Wi-Fi networks were very vulnerable to cyber-attacks mostly because of their borderless nature. Public hotspot users were more prone to cyber-attacks because such attacks were usually passive and users were unaware of them.
Purkait, 2012	Literature Review	16 dissertations and 358 papers		Internet users' trust have been negatively impacted by phishing attacks. Phishing awareness training was recommended to reduce the negative impacts.
Purkait et al., 2014	Empirical investigation	621 Internet users with some experience with online financial transactions	Survey and three experimental tasks: Awareness on phishing, safe Internet practices, Internet skill, vigilance, memory, and ability to	Developed a model to investigate the factors which have significant impacts on the ability of Internet users to correctly identify a phishing website. Phishing awareness training was encouraged as it had a significant positive

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			identify phishing website	effect on the ability of users to identify phishing websites.

Cybersecurity Awareness

Rahim et al. (2015) stated that cybersecurity awareness involved “alerting Internet users of cybersecurity issues and threats, and enhancing Internet users’ understanding of cyber threats so they can be fully committed to embracing security during Internet use” (p. 607). Cybersecurity awareness has, therefore, been posited as a means of reducing the effects of cyber-attacks on Internet users as it notifies them of cyber-attacks, and increases their understanding of how to mitigate the effects of such attacks (Choo, 2011; Rahim et al., 2015). For example, cybersecurity awareness was found to empower Internet users with the ability to detect and avoid cyber-attacks (Kritzinger & von Solms, 2010), improve cautious actions of users when using the Internet (McCrohan et al., 2010), and positively influence the ability to detect cyber-attacks as well as motivate secure Internet use (Claar & Johnson, 2012). Further support has been established in literature for the view that cybersecurity awareness increases the users’ abilities to detect cyber-attacks, and hence, will take mitigating actions (Albrechtsen & Hovden, 2010; D’Arcy et al., 2009; White, 2015; Wolf et al., 2011). At the same time, however, White (2015) also found that an increase in a user’s cybersecurity awareness also increased the number of reported cybersecurity incidents, while Wolf et al. (2011) found that the effectiveness of cybersecurity awareness diminished over time. D’Arcy et al. (2009)

found that security education, training, and awareness (SETA) programs led to a reduction in the misuse of IS among computer users. SETA programs provide users with general security knowledge to raise their awareness levels as well as the necessary skills on how to carry out any required security actions (D'Arcy et al., 2009; Whitman, 2003). However, although SETA programs should raise the awareness and security skills levels of users, limited cybersecurity skills have been reported as one of the biggest challenges in cybersecurity (Abawajy, 2014; Adams & Makramalla, 2015; Ramim & Levy, 2006). Further, Abawajy (2014) indicated that an increased concentration of users' cybersecurity awareness was necessary to decrease human-related InfoSec threats. According to Tsohou, Kokolakis, Karyda, and Kiountouzis (2008), the goal of cybersecurity awareness should be to inculcate a consciousness of security in Internet users which should ultimately manifest in them exhibiting more secure actions while online. Therefore, cybersecurity awareness should be the first step in acquiring cybersecurity skills as its focus is to attract the users' attention to the more important issue of getting to know how to respond to cybersecurity threats (Tsohou et al., 2008). Slusky and Partow-Navid (2012) as well as Abawajy (2014) emphasized that cybersecurity awareness training should be context-aware, that is, its content should include cybersecurity risks and safe practices that are specific to the users. Further, for the cybersecurity awareness goal to be achieved, it has been recommended that Internet users should be divided into specific target groups such as by age, and by type of users, example HCUs, so that the right content can be conveyed to the right group (Choo, 2011; Furnell, 2008; Peltier, 2005). Additionally, Kim (2014) suggested that the cybersecurity awareness levels of users should be measured prior to training such that the content of the training can be current to

the users' needs. Moreover, the content should be in the form of real-life scenarios including pictures and stories to make it more appealing as well as interesting to the specific target group (Kim, 2014; McCrohan et al., 2010; Rahim et al., 2015). Similarly, Choi (2013) as well as Rezgui and Marks (2008) emphasized the importance of making cybersecurity awareness training appealing to users, as users tend to be more interested in taking the training if they knew the significance of such awareness in protecting themselves and their computers from cybersecurity threats. Additionally, Abawajy (2014) found that users preferred when a combination of delivery methods is used to deliver the cybersecurity awareness training, instead of using a single method. Based on the preceding discussion, it appears that further investigation into the effectiveness of cybersecurity awareness is warranted. Therefore, this study targeted senior citizens, measured their cybersecurity awareness levels and their cybersecurity skills, among other things, prior to, and after, cybersecurity awareness training, as well as used real-life scenarios to convey the cybersecurity awareness content. Similar to Abawajy (2014), the training was delivered using a combination of methods such as video-based, text-based, that is, PowerPoint presentation, and instructor-led explanations. This also shed more light on the effectiveness of cybersecurity awareness as well as determined if it contributed to the motivation of the senior citizens to acquire cybersecurity skills, among other things. Additionally, to have the desired effect of empowering the senior citizens to identify and mitigate the effects of cyber-attacks, the training content also focused on what they needed to know about cybersecurity threats, rather than what was nice to know (Kim, 2014).

Table 5

Summary of Cybersecurity Awareness-related Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Abawajy, 2014	Exploratory study using experiments	60 participants	Questionnaire and manual scoring: InfoSec awareness delivery methods (text-based, game-based & video-based)	InfoSec awareness training is a very effective way to empower users with the requisite knowledge on InfoSec topics. A combined InfoSec training delivery method is better than using different training methods separately.
Albrechtsen & Hovden, 2010	Empirical investigation (quantitative and qualitative)	197 employees	Survey, interviews, group discussions and observations: User awareness and user behaviour	Positive changes in InfoSec awareness and behaviour can be achieved through employee participation, collective reflection and group interactions.
Claar & Johnson, 2012	Empirical Investigation	184 Internet users	Online survey: Perceived vulnerability, perceived severity, perceived benefits, perceived barriers, self-efficacy, cues to action, and computer security usage	Demonstrated that the Health Belief Model can be used to study computer security usage behavior of HCU's and what motivates them to protect their computer systems.
D'Arcy et al., 2009	Empirical Investigation	269 computer users from eight different companies	Questionnaire: User awareness of security policies, SETA programs, computer monitoring,	Deterrence theory is applicable in the InfoSec domain. User awareness of security policies, SETA programs, and computer

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			perceived certainty, severity of sanctions, and IS misuse intention	monitoring deter IS misuse. Perceived severity of sanctions is more effective in reducing IS misuse than certainty of sanctions.
Kim, 2014	Empirical investigation	68 students (undergraduate & graduate) in a mid-sized university.	Questionnaire: Attitudes toward information security awareness	Information security awareness training (ISAT) should be comprehensive so that students can know what and how to effectively protect their systems and information. ISAT should be repeated regularly to counter new security issues.
Kritzinger & von Solms, 2010	Theoretical model development			Proposed the E-Awareness Model as a way to improve cybersecurity awareness among HCUs before they ventured into cyberspace.
McCrohan et al., 2010	Empirical Investigation	396 university undergraduate business school students	Questionnaire: Cyber threat education and awareness, user security behavior	Increased cybersecurity awareness resulted in a positive effect on online security actions of participants.
Rahim et al., 2015	Literature Review	24 articles from academic journals		Proper categorizing of Internet users and cybersecurity awareness programmes are critical for effectiveness in order for the right

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				cybersecurity message to be conveyed to the right audience.
Rezgui & Marks, 2008	Interpretive case-study	45 employees from the Computer Science department at a university	Questionnaires, interviews, documentation, and observations: InfoSec awareness	Employees' InfoSec awareness, behaviour and work attitude were affected by factors such as conscientiousness, cultural assumptions and beliefs, as well as social conditions.
Slusky & Partow-Navid, 2012	Empirical investigation	340 university students	Survey: IT resources and skills, InfoSec practices and awareness, InfoSec awareness training	Compliance with InfoSec awareness was lower than the users' understanding of it. Users had good knowledge of InfoSec awareness, but struggled with the application of the knowledge in real-world situations.
Tsohou et al., 2008	Literature review	48 information security awareness studies	Security awareness strategies, e.g. campaigns, practices, programs, research studies, InfoSec standards, surveys and reports	No clarification exists on many security concerns, hence security researchers, practitioners and managers were frustrated on security awareness efforts.
White, 2015	Empirical investigation	945 participants	Online survey: Education of computer security, preventative behaviour, and security	Security incidents were not lowered by the implementation of technology. Focus should be on the people who use the

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			outcomes (security incidents & security prior knowledge)	technology. A negative relationship existed between education and preventative behavior with the number of reported security incidents.
Wolf et al., 2011	Empirical investigation / experiment	122 adults consisting of faculty and staff at a K-12 educational institution	Software, e.g. extracting password hashes from the school's user accounts on one of the active directory domain controller servers: password policy compliance	Best to use hardware or software to enforce password policy. Provided a clear and concise definition of security awareness.

Cybersecurity Skills

Cybersecurity awareness training is essential, however, it did not provide the necessary skills training that users needed to better protect themselves against cyber-attacks (Adams & Makramalla, 2015; Tsohou et al., 2008). As previously noted, cybersecurity awareness should, rather, be the first step in acquiring cybersecurity skills as, by itself, it has been reported to be insufficient in conveying the required skills for users to reduce the success of cyber-attack vectors (Adams & Makramalla, 2015; Tsohou et al., 2008). According to Carlton and Levy (2015), “cybersecurity skills correspond to an individual’s technical knowledge, ability, and experience surrounding the hardware and software required to execute information security in protecting their IT against

damage, unauthorized use, modification, and/or exploitation” (p. 3). Skill is a combination of knowledge, experience, and ability that enable end-users to perform a task well (Boyatzis & Kolb, 1991; Levy, 2005). It has been consistently reported in literature that limited cybersecurity skills amongst Internet users is one of the biggest challenges of cybersecurity, and can result in significant financial losses to the users (Abawajy, 2014; Adams & Makramalla, 2015; Ramim & Levy, 2006). Therefore, investing in the acquisition of cybersecurity skills should reduce the financial burden on users from the cyber-attacks (Adams & Makramalla, 2015). Limited cybersecurity skills have also been identified as one of the leading contributors to human vulnerabilities to cybersecurity threats, for example, phishing attacks, which in turn accounts for 80% of total vulnerabilities that are often exploited by cyber-attackers (Adams & Makramalla, 2015; Nagarajan, Allbeck, Sood, & Janssen, 2012). IS users, especially those who use the Internet need the appropriate and relevant skills set in order to effectively use the ever-changing technological innovations and counter the associated cybersecurity threats (Choi, 2013; Lerouge, Newton, & Blanton, 2005). Cybersecurity skills training aims to instill the required skills that are necessary to mitigate the effects of the growing numbers of cyber-attacks and should not be limited to IT professionals (Adams & Makramalla, 2015; Nagarajan et al., 2012). Carlton and Levy (2015) identified the top nine cybersecurity skills that are needed by non-IT professionals, and emphasized the development of those skills to counter cyber-attacks. Evidence from research has also indicated that when Internet users have high levels of cybersecurity knowledge and skills, they were more motivated to play active roles towards countering cybersecurity threats such as identity theft (Holt & Turner, 2012; Inan et al., 2016; Mohamed & Ahmad,

2012). Additionally, it has been argued that users who lack cybersecurity skills and underestimate the dangers inherent in their actions represent a huge risk in cybersecurity, however, this risk can be mitigated by effective cybersecurity awareness and skills training programs (Choi, 2013; Rezgui & Marks, 2008).

Table 6

Summary of Cybersecurity Skills-related Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Adams & Makramalla, 2015	Literature review and analysis		Training scenarios using gamification, entrepreneurial perspectives, cyber-attackers, and their characteristics	Recommended that organizations should invest in building cybersecurity skills in all employees including those in leadership. Proposed using gamification methods in cybersecurity skills training, which, enabled employees across all levels to play the roles of various types of attackers.
Carlton & Levy, 2015	Developmental study	18 cybersecurity and subject matter experts	Questionnaire; Cybersecurity threats and related skills	Identified the top nine platform independent cybersecurity skills required by non-IT professionals to mitigate the top cybersecurity threats faced by organizations.
Choi, 2013	Empirical investigation	185 professionals working at a government agency	Internet-based survey: Cybersecurity threats and vulnerabilities	Computer misuse intentions of end-users can be reduced through increased

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Lerouge et al., 2005	Empirical investigation	124 systems analysts in Fortune 500 companies	Survey: System development tasks skills, political skills, interpersonal skills, business task knowledge, technology skills	cybersecurity skills. To exploit technology innovations in an effective manner, all IS employees need an appropriate skill set. Systems analysts recognize all investigated skills as important to their role.
Levy, 2005	Empirical investigation	Two MBA programs (one online & one on campus)	Questionnaire: Learning skill profile	Skills were enhanced in the two MBA programs
Nagarajan et al., 2012	Analysis		Gamification	Cybersecurity skills training that focus mostly on the theoretical security knowledge and lack the hand-on aspect will not be as effective. Such skills training should require participants to both think and apply the theoretical knowledge in real-time; highly interactive video games can help to achieve this goal.
Torkzadeh & Lee, 2003	Empirical investigation	282 professional employees and managers (first, middle, and top)	Questionnaire: Perceived end-user computing skills	Developed and validated a 12-item instrument for measuring perceived end-user computing skills.
Tsohou et al., 2008	Literature review	48 information security awareness (ISA) studies	ISA strategies, e.g. campaigns, practices, programs, research	ISA did not provide users with cybersecurity skills: it is the first

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			studies, information security standards, surveys and reports	level of a security learning pyramid.

Risk and Risk Mitigation

Definition and Types of Risks

Risk has been viewed as a complex concept that has caused a lot of ambiguity and as such, been studied from several disciplinary perspectives, including decision science, behavioral economics, psychology, and marketing (Featherman & Wells, 2010; Gerber & von Solms, 2005). Within the InfoSec domain, NIST (2011) defined risk as:

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (p. B-8)

Risk has also been identified as a critical factor that influences the decisions and actions of individuals in that it “affects individual decision-making when the decision may produce adverse consequences over which the individual has no control” (Featherman & Wells, 2010, p. 113). Yazdipour and Neace (2013) indicated that several researchers have studied risk from the perspective of it being a perception, i.e. risk is subjective, rather than it being an objective scientific/statistical property, and hence, should be distinguished from the traditional economic perspective.

Perceived Risk

Nemati and Van Dyke (2009) defined perceived risk as “a person’s belief in the likelihood that they will be harmed as a consequence of taking a particular action” (p. 52). Perceived risk is also known to refer to the belief that an individual has regarding uncertainty and consequences in a given situation (Brewer, Chapman, Gibbons, Gerrard, McCaul, & Weinstein, 2007; Carvalho, Block, Sivaramakrishnan, Manchanda, & Mitakakis, 2008; Lu, Hsu, & Hsu, 2005). Consequently, an individual’s perception of risk will largely depend on how the individual interprets a situation at hand, and this will ultimately determine the actions that the individual will take towards the risk (Carvalho et al., 2008). An individual’s perception of risk is considered to be a key element to how the individual evaluates options, makes choices and acts (Campbell & Goodstein, 2001; Liao, Lin, & Liu, 2010). Therefore, perceived risk appears to be a relevant construct when investigating the actions of individuals. Additionally, it has been argued that during the decision-making process, uncertainty will produce a higher level of “psychological discomfort,” which should ultimately motivate the decision-maker to take mitigating actions that will reduce the discomfort, and hence reduce the uncertainty in the situation (Yazdipour & Neace, 2013). There is also evidence from literature to indicate that there is a relationship between the levels of a user’s perceived risk and the motivation to take actions to mitigate the risks (Herath & Rao, 2009; Johnston & Warkentin, 2010; Lee & Larsen, 2009; Liang & Xue, 2010; Workman et al., 2008). For example, Workman et al. (2008) indicated that perceived risk influenced a user’s risk related actions, hence, the user will take mitigating actions. However, Workman et al. (2008) also noted that users do not always take known mitigating actions to protect their information because the

level of the user's perceived risk, influences how motivated the user will be to take the necessary mitigating actions. The findings of Johnston and Warkentin (2010) also suggest that when users were made aware of risks regarding cybersecurity threats, the users were more motivated to take mitigating actions. However, Liang and Xue (2010) found a negative interaction between the levels of a user's perceived risk and the user's motivation to take mitigating actions. Therefore, the preceding contradicting reports from literature indicate that further research is necessary to investigate the relationship between perceived risk and motivation to mitigate the risk.

Prior research has investigated perceived risk as a multi-dimensional construct that uses the types of risk that are considered to be relevant to a given context (Jacoby & Kaplan, 1972; Liao et al., 2010; Lu et al., 2005; Stalker, 2012). This suggests that the context within which perceived risk is studied will determine the type of risk that is investigated. There are eight commonly studied dimensions of perceived risk, namely, performance, financial, social, psychological, security, privacy, physical, and time (Featherman & Pavlou, 2003; Jacoby & Kaplan, 1972; Liao et al., 2010; Lu et al., 2005). For example, Featherman and Wells (2010) investigated the relationship between users' perceived risks and their decision to use an e-service. Within that context, Featherman and Wells (2010) investigated the following risk dimensions: performance, financial, privacy, time, psychological, and social. Also, Hanafizadeh and Khedmatgozar (2012) investigated if bank customers' awareness of Internet banking services and its advantages were effective in reducing the negative effects that the customers' perceived risks had on their use of the banking services. In that context, the following dimensions of risk were studied: time, financial, performance, social, security, and privacy. Further, Zhao,

Hanmer-Lloyd, Ward, and Goode (2008) identified the risk factors that would discourage consumers in China from using the Internet banking service. In that context, the following dimensions of risk were studied: performance, security, financial, privacy, time, psychological, social, and physical. Similar to Zhao et al. (2008) and within the context of this study, all eight commonly studied dimensions of perceived risk were explored, as all were believed to be relevant to the motivation to take actions to mitigate cyber-attacks.

Performance risk refers to the efficiency of a product or the probability that it may malfunction and might not perform as expected (Featherman & Pavlou, 2003; Hanafizadeh & Khedmatgozar, 2012; Liao et al., 2010; Lu et al., 2005). Within the context of this study, performance risk is defined as a senior citizen's perception that the Internet may malfunction and not work properly when it is used. Financial risk refers to any financial or monetary damage or loss that may be incurred from acquiring a product (Featherman & Pavlou, 2003; Liao et al., 2010; Lu et al., 2005). Within the context of this study, financial risk is defined as a senior citizen's perception that his/her identity will be stolen while using the Internet, and hence, will suffer financial loss. Loss of all life savings which can result in billions of dollars was one of the reported devastating effects of identity theft on senior citizens (Holt & Turner, 2012; Jones, 2001). Social risk refers to the potential loss of a person's standing within a social group as a result of using a product, i.e. the probability that the person will perceive that he/she will look foolish to other people that he/she considers to be important (Featherman & Pavlou, 2003; Lu et al., 2005). Within the context of this study, social risk is defined as a senior citizen's perception that social status will be lost if persons in his/her social group know that

his/her identity was stolen while he/she was using the Internet. This indicates that there will be significant changes in the lifestyle of the senior citizen if there is identify theft that results in financial loss. Psychological risk refers to a user's perception of the potential loss of self-esteem, peace of mind, mental stress, or self-perception/ego that results from worrying or feeling frustrated when a product is used (Featherman & Pavlou, 2003; Liao et al., 2010; Lu et al., 2005). Within the context of this study, psychological risk is defined as a senior citizen's perception that he/she will suffer mental stress or not have peace of mind when he/she uses the Internet for fear of being a victim of identity theft. Jones (2001) indicated that after having their identity stolen via Internet use, some senior citizens suffered devastating effects, for example, feelings of shame for being victims. Security risk refers to concerns that users have regarding potential cyber-attacks on the networks and data transactions during the sending/receiving of financial information online, including but not limited to, network hacks as well as unauthorized access to their financial accounts via false identification (Hanafizadeh & Khedmatgozar, 2012; Maditinos, Chatzoudes, & Sarigiannidis, 2013). Within the context of this study, security risk is defined as a senior citizen's concerns regarding potential loss that can result from using networks that do not have adequate security which can result in fraudulent activities by cyber-criminals such as identity theft. Privacy risk refers to the "potential loss of control over personal information, such as when information about you is used without your knowledge or permission" (Featherman & Pavlou, 2003, p. 455). This includes instances where Internet users' PII is unknowingly collected and registered as well as when cyber-criminals use the PII to commit acts of financial fraud, for example, identity theft (Featherman & Wells, 2010; Hanafizadeh & Khedmatgozar,

2012). Within the context of this study, privacy risk is defined as a senior citizen's perception of the loss of privacy and confidentiality to his/her PII which can result in identity theft online. Physical risks "involves the potential threat to an individual's safety, physical health and wellbeing" (Lu et al., 2005, p. 109). Within the context of this study, physical risk is defined as any threat to a senior citizen's physical health because of having his/her identity stolen. Jones (2001) reported that some senior citizens suffered exacerbated illnesses that sometimes lead to premature deaths after having their identity stolen via Internet use. Time risk refers to the "potential losses to convenience, time and effort caused by wasting time researching, purchasing, setting up, switching to and learning how to use the e-service" (Featherman & Wells, 2010, p. 114). Internet users may perceive that they are wasting time if it will take too much time to learn how to participate in online activities and also to solve problems that may be caused from participating in those activities, e.g. to resolve issues that arise as a result of identity theft (Aldás-Manzano, Lassala-Navarré, Ruiz-Mafé, & Sanz-Blas, 2009; Hanafizadeh & Khedmatgozar, 2012). Within the context of this study, time risk is defined as any loss of time incurred by a senior citizen because of having to expend extra effort to learn how to protect himself/herself from identity theft, and to resolve any issues that may arise if identity theft occurs while using the Internet.

Featherman and Pavlou (2003) also measured overall risk after measuring the different dimensions of perceived risk. Overall risk is "a general measure of perceived risk when all criteria are evaluated together" (Featherman & Pavlou, 2003, p. 455). Thus, after assessing all the aforementioned eight dimensions of perceived risk, this study also calculated the overall perceived risk. Various models have been used to calculate overall

risk, however, the additive and multiplicative models have been the two most commonly used models (Bettman, 1973; Dowling, 1986; Yazdipour & Neace, 2013). Bettman (1973) as well as Yazdipour and Neace (2013) reported that it appeared that when the additive models were used to calculate overall risk, more variability in perceived risk was explained than when the multiplicative models were used. Further, several studies have used the additive model to calculate overall perceived risk and have found good results (Bettman, 1973; Dowling, 1986; Featherman & Pavlou, 2003). Therefore, this study used the additive model to calculate overall risk.

Table 7

Summary of Perceived Risks-related Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Aldás-Manzan et al., 2009	Empirical investigation	511 Internet banking service users	Survey: Perceived risk (PR) dimensions (Performance, security, social, privacy, & time loss), consumer innovativeness, and Internet banking service use	Provided a model that integrated consumer innovativeness traits influence with the perception of adoption risks on the acceptance of Internet banking services. Perceived risk greatly inhibits Internet banking use.
Bettman, 1973	Empirical investigation	123 housewives in Los Angeles	Questionnaire; Inherent risk, handled risk, mean quality, percentage acceptable, relative variance, importance, perceived price, mean familiarity,	Similar results were yielded by additive and multiplicative risk models. Consumer choice was influenced by perceived risk. Distinguished between inherent and handled risk models.

Study	Methodology	Sample	Instrument or Construct information, usefulness, and confidence	Main Findings or Contributions
Brewer et al., 2007	Meta-analysis	34 articles		The perceptions of risk construct significantly influence health behaviour. Therefore, this construct should be included in health-behaviour theories to improve their abilities to predict health behaviours.
Campbell & Goodstein, 2001	Empirical investigation	Study 1: 67 managers in an MBA program, study 2: 171 undergraduate students, study 3: 147 MBA students	Scenarios and survey: PR, incongruity, and consumer evaluation	Consumers consider the risk that is associated with a product when evaluating moderately incongruent products. When high risk is present, the moderate incongruity effect is reversed, but can be eradicated by relatively low risk. This can happen when the product evaluation does not involve any risk.
Feather & Wells, 2010	Empirical investigation	234 undergraduate business students	Survey: Mental intangibility, PR dimensions (performance, financial, social, privacy, psychological & time), perceived ease of use, perceived usefulness, and intent to use	Re the e-service, financial, privacy, and performance risks were most affected by the mental intangibility experience of consumers. Only in cases where the consumers had a clear mental picture of the e-service, did the perceived ease of

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				use of the e-service acted as a risk-reducing factor.
Featherman & Pavlou, 2003	Empirical investigation	Undergraduate business students of a large university. Sample 1: 214, sample 2: 181	Survey; PR dimensions (financial, privacy, time, psychological, social, & performance; overall risk), usefulness, ease of use, and adoption intention	Performance-based risk perceptions, and perceived ease of use of the e-service were the two variables that primarily adversely affected the e-service adoption.
Gerber & von Solms, 2005	Analysis			Proposed a comprehensive integrated approach to analyze risk to both tangible and intangible asset.
Hanafizadeh & Khedmatgozar, 2012	Empirical investigation	554 bank customers who did not actively use the Internet Banking (IB) service	Questionnaire: PR dimensions (time, social, financial, performance, security, & privacy), IB awareness, intention to use	All PR dimensions except social risk, had significant negative effects on IB use. IB awareness reduced all aspects of PR dimensions. IB awareness had a significant role in increasing the intention of using IB.
Jacoby & Kaplan, 1972	Empirical investigation	148 university students	Questionnaire: PR dimensions: (physical, social, financial, performance, psychological, & overall)	Construct and predictive validity were demonstrated in the results. Five dimensions of PR predicted well the overall perceived risk, namely, financial, performance,

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Johnston & Warkentin, 2010	Experiment; model development	275 participants (faculty, staff, & students from a large university)	Survey: Protection Motivation Theory (PMT), social influence, self-efficacy, response efficacy, threat severity, threat susceptibility and behavioral intent	physical, psychological, and social risk. The behavioral intentions of users to comply with security recommendations were impacted by fear appeals. Developed, validated and found good support for the fear appeal in that it contextualizes the PMT danger control process in the technology adoption literature.
Lee & Larsen, 2009	Empirical investigation	239 small and medium sized business (SMB) executives (IT executives, CEO, CFO, & COO) from various industries	Questionnaire: Self-efficacy, response efficacy, response cost, perceived severity, perceived vulnerability, social influence, vendor support, IT budget, firm size, and adoption intention	Developed and validated a model based on PMT that explained a significant amount of variance in SMB software adoption. The SMB executives' intent to adopt anti-malware software were significantly affected by the threat and coping appraisal variables.
Liang & Xue, 2010	Empirical investigation and model development	152 university business students	Questionnaire: Perceived susceptibility, perceived severity, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy,	Developed and tested a model based on Technology Threat Avoidance Theory. Higher levels of perceived threat were associated with weaker relationships between avoidance

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			avoidance motivation, and avoidance behavior	motivation and safeguard effectiveness. IT threat avoidance behavior of users were predicted by their avoidance behavior, which were ultimately determined by self-efficacy, safeguard effectiveness and cost, as well as perceived threat.
Liao et al., 2010	Empirical investigation	305 participants	Web-based survey: Perceived performance risk, perceived social risk, perceived prosecution risk, perceived psychological risk, subjective norm, perceived behavioral control, attitude, and intention	Attitude towards using pirated software was strongly predicted by perceived psychological risk. Intention to use pirated software was impacted by perceived prosecution risk, attitude, and perceived behavioral control.
Lu et al., 2005	Empirical investigation	1259 registered online antivirus application (OLA) users	Survey: PR dimensions (financial, social, time loss, physical, functional, opportunity cost, & information), perceived ease of use, perceived usefulness, attitude towards using,	Behavioral intention to use an OLA that is under information security threats is indirectly affected by PR. Trial users of the OLA were less influenced by PR than those who had continued to use it.

Study	Methodology	Sample	Instrument or Construct and behavioral intention to use	Main Findings or Contributions
Workman et al., 2008	Empirical investigation	588 employees from a large technology-oriented services corporation	Online questionnaire and observations: Perceived severity, vulnerability, locus of control, self-efficacy, response efficacy, response cost, subjective omissive behavior, and objective omissive behavior	Proposed the threat control model to explain the knowing-doing gap in InfoSec. Users' perception of the severity of a threat will dictate their motivation level to avert the threat.
Yazdipour & Neace, 2013	Literature review and model development		Total perceived risk, resident risk, behavioral risk, psychological discomfort and risk attitude	Developed the Behavioral Finance Risk Model that proposed that perceived risk was a function of the comfort level of the decision maker when comparing one business venture over other such opportunities.
Zhao et al., 2008	Exploratory study	432 university students in southern China who used the Internet	Questionnaire: PR dimensions (performance, security, financial, privacy, time, psychological, social, & physical), consumers' comprehension of the Internet banking services (IBS),	There is value in using PR to explain the decision of the consumers on whether to use IBS. The more important PR dimensions that prevented the use of the IBS were privacy, finance, security, and performance. Barrier to risks that

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			and behavioral intention to use the IBS.	were identified were influenced by culture.

Perceived Risk of Identity Theft

Identity theft is a crime that occurs when a person unlawfully uses another person's PII for personal gain, for example, to obtain financial benefits, or, with the intention to commit fraud or other crimes (Bellah, 2001; Lai et al., 2012). Therefore, within the context of this study, perceived risk of identity theft is an Internet user's belief in the likelihood of another person unlawfully using his/her PII for personal gain while he/she is online. The increased use of the Internet by senior citizens for services such as e-commerce (e.g. online shopping), and financial services (e.g. online banking) put them at greater risks to have their identity stolen (Grimes et al., 2010; Holt & Lampke, 2010; Holt & Turner, 2012; Morris, 2010). This is due to the fact that these online services require the senior citizens to transit sensitive personal and financial information via the Internet, which can then be stolen by cyber-criminals through methods such as phishing (Holt & Lampke, 2010; Holt & Turner, 2012). According to Roberts et al. (2013), perceived risk of identity theft "is now greater than worry about many traditional place based crimes" and as such "represents a significant threat to the free movement and quality of life of citizens in the 21st century" (p. 323). Prior research had indicated that identity theft is one of the common risk perceptions of senior citizens when they use the Internet, and coupled with their limited cybersecurity skills, they feel overwhelmed, frustrated as well as demotivated when they use the Internet (Greengard, 2009; Jones,

2001). Further, in spite of the limited knowledge of cybersecurity skills amongst senior citizens which make them more prone to cyber-attacks, they were still less likely to take actions to protect themselves against such attacks, e.g. identity theft (Grimes et al., 2010). Grimes et al. (2010) indicated that increasing the senior citizens' cybersecurity skills should minimize their perception of risks. Conversely, this suggests that the level of senior citizens' perceived risk of identity theft should contribute to their motivation to acquire cybersecurity skills to mitigate the risks. Workman (2008) found that "carelessness with information and failure to take available precautions contributes to the loss of information and even to crimes such as corporate espionage" (p. 475). Lai et al. (2012) also reported that users who had low perceptions of risks would likely not be as careful with protecting their PII, and hence, were at greater risk of identity theft. Therefore, within the context of this study, it was inferred that if senior citizens were careless with their PII while online, and failed to take the necessary precautions, then their PII could be compromised, resulting in identity theft. Holt and Turner (2012) indicated that even though there was significant growth in the prevalence and impact of identity theft-based crimes, very little was known about the persons who were identified as high risk and how they can protect themselves from such crimes in cyberspace. Similarly, Henson, Reynolds, and Fisher (2013) stated that there was limited report in the literature regarding perceived risk within the cyberspace environment. Therefore, Henson et al. (2013) called for further research in this area, especially since opportunities for cybercrimes such as identity theft increase with the innovations in technology.

Table 8

Summary of Perceived Risk of Identity Theft-related Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Grimes et al., 2010	Empirical Investigation	Sample 1: 120 participants between 30 and 91 years old. Sample 2: 47 students between 19 and 57 years old	Survey: Computer use, interest, and expertise; privacy and trust; and Internet security awareness	Protecting the private information of older adults is very important because they were specifically targeted online for financial crimes.
Henson et al., 2013	Exploratory study	838 undergraduate students from a large university	Web-based survey: Fear of online interpersonal victimization (OIPV), perceived risk of OIPV, previous online victimization, and online exposure	Educational programs for OIPV are needed because participants were not taking the necessary precautions to defend themselves against online victimization. Fear of OIPV for all types of victim-offender relationships was significantly related to perceived risk of OIPV. Previous online victimization was significant for fear of OIPV by intimate partners and friends/acquaintances only.
Holt & Lampke, 2010	Exploratory study	300 threads from six web forums for the sale and exchange of identity information	Identity theft, compromised banks, eBay, and PayPal accounts	Various personal and financial data, e.g. credit card, bank account information, and PII were available online at a fraction of their true value. Distinct relationships existed between buyers and sellers that shape the associations and

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				structure of online data theft markets.
Holt & Turner, 2012	Empirical investigation	602 university students, faculty, and staff	Survey: Resiliency from on-line identity theft, risk factors, and protective factors	Significant positive relationship existed between on-line victimization and risk. Resiliency to victimization was increased by protective software programs.
Lai et al., 2012	Empirical investigation	117 undergraduate students of a public university in the U.S.	Questionnaire: Identity theft, conventional coping, technological coping, self-efficacy, perceived effectiveness, and social influence	Occurrences of identity theft can be reduced by both conventional and technological coping. Self-efficacy, perceived effectiveness of coping, and social influence all had significant impacts on technological coping.
Morris, 2010	Analysis and review	257 news articles on identity theft cases for the period 1995 to 2005	Identity theft categories (circumstantial, general, sophisticated, & highly sophisticated)	Most cases of identity theft were financially motivated; reported identity theft cases were those that were minor in nature; offenders varied in both age and gender.
Roberts et al., 2013	Exploratory study	1,550 Internet users	Fear of cyber-identity theft and predictors of fear (traditional & Internet crimes)	A generalized fear of crime and a specific Internet exposure were the predictors of fear of cyber-identity theft.

Computer Self-Efficacy (CSE)

Self-efficacy (SE), which is grounded in social psychology refers to the beliefs that a person has in his/her ability to perform a particular activity, and has been identified as a construct which influences individual effort as well as motivation (Bandura, 1986; Compeau & Higgins, 1995; Gist, 1987; Marakas, Johnson, & Clay, 2007). This suggests that since SE impacts how an individual feels, thinks or acts, the level of an individual's SE can impede or boost the individual's motivation to act (Bandura, 1986; Kumar & Kadiravan, 2012). Compeau and Higgins (1995) extended the SE concept to introduce computer self-efficacy (CSE) which is defined as "an individual's perceptions of his or her ability to use computers in the accomplishment of a task" (p. 191). Therefore, within the InfoSec domain, CSE is a more focused construct than SE because it refers to an individual's perceptions of his/her capabilities to competently use computers to perform an activity (Bhatnagar, Madden, & Levy, 2016; Compeau & Higgins, 1995).

Understanding the factors that influence a person to act towards computer technologies has always been a key goal in IS research, and CSE has been identified as an important variable in predicting how users will act (Compeau & Higgins, 1995; Levy & Danet, 2010; Marakas et al., 2007). Since CSE includes feelings of confidence, then, enhancing users' CSE should positively contribute to the users' usage of computer technologies (Cassidy & Eachus, 2002; Igarria & Iivari, 1995; Laganá et al., 2011; Marakas, Yi, & Johnson, 1998). Thus, CSE is an important and extensively used construct in IS research, and it has repeatedly been found to have significant impact on a wide range of cognitive and behavioral outcomes (Karsten, Mitra, & Schmidt, 2012; Kher, Downey, & Monk, 2013; Marakas et al., 1998). Numerous IS researchers have investigated the role of CSE

within the IS domain, for example, the moderating role of CSE in predicting the continuance usage of e-learning systems was investigated and it was concluded that CSE did not significantly influence learning outcomes (Hayashi, Chen, Ryan, & Wu, 2004); CSE was found to have a significant influence on learning performance and the suggestion was made that it was important to evaluate the self-efficacy beliefs of trainees prior to computer training as well as enhance their perceptions of CSE (Hasan & Ali, 2004); support was found for the hypothesis that users with higher CSE were less influenced by security countermeasures (D'Arcy & Hovav, 2009); and it was found that CSE significantly predicted motivation to learn computing skills (Zhang & Espinoza, 1998). According to Phipps et al. (2013), to sustain motivation in acquiring new skills, an adequate level of SE is required. Therefore, within the InfoSec context, an adequate level of CSE should contribute to the motivation of Internet users to acquire cybersecurity skills to mitigate the effects of cyber-attacks. Rhee et al. (2009) also indicated that training programs that enhanced CSE could lead to users exhibiting a higher level of security effort and awareness.

Table 9

Summary of CSE-related Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Bhatnagar et al., 2016	Empirical Investigation	140 participants	Survey: CSE, ethical severity of misusing IS (ESMIS), resistance to use IS, and IS usage	IS usage was not significantly influenced by ESMIS. CSE exhibited a significant negative contribution to IS usage but had no

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				contribution to ESMIS.
Boss et al., 2009	Empirical Investigation	1671 users from a large medical center in southeastern US	Survey: Specification, evaluation, rewards, mandatoriness, and precaution. Control variables: CSE and apathy	CSE was important in influencing InfoSec behaviors. Users with high CSE displayed better understanding of knowledge in protecting corporate computer assets.
Cassidy & Eachus, 2002	Empirical investigation	Sample 1: 101 university students; Sample 2: 212 university students	Survey: CSE, computer user self-efficacy (CUSE), gender, and experience with computers	Developed and validated a 30-item instrument to measure CUSE; significantly higher levels of CSE observed in males than females; significant positive correlations between computer experience and CSE; increased CSE observed in participants who owned a computer and received computer training.
Compeau & Higgins, 1995	Empirical investigation	1020 knowledge workers, mostly managers	Questionnaire: Encouragement by others, others' use, support, CSE, outcome expectations, affect, anxiety, and usage	Developed and validated a 10-item CSE measurement instrument. SE had the most value in understanding

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				why people use computers.
D'Arcy & Hovav, 2009	Empirical investigation	Group 1: 238 employed professionals taking evening MBA classes; Group 2: 269 employees in eight organizations located across the U.S.	Survey: Unauthorized access, unauthorized modification, CSE, virtual status, user awareness of SETA programs, security policies, and computer monitoring	CSE had a negative effect on the relationship between SETA programs and unauthorized access intention. No moderating effect of CSE on the impact of SETA on unauthorized modification. SETA did not have a direct effect on unauthorized modification.
Gist, 1987	Literature review			Self-efficacy impacted persistence, task effort, expressed interest, and the level of difficulty for goal performance.
Hasan & Ali, 2004	Empirical investigation	151 undergraduate students	Survey: CSE, learning performance, computer experience and computer attitude	CSE and computer experience had positive and direct effects on learning performance. Computer attitudes had indirect impact on learning performance but this was only through their direct effect on CSE.
Hayashi et al., 2004	Field Experiment	110 college undergraduate	Questionnaire: Perceived usefulness, confirmation,	No significant relationship existed among the

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
		Business students.	satisfaction, IS continuance, and CSE	CSE of online learners, confirmation, satisfaction, and their perceived usefulness. As a moderating variable, CSE did not significantly influence learning outcomes.
Igbaria & Iivari, 1995	Empirical investigation	450 computer users	Computer experience, organizational support, SE, computer anxiety, perceived ease of use, perceived usefulness, and system usage	CSE is negatively related to anxiety, but had both direct and indirect effects on system usage. Computer experience had a strong positive direct effect on CSE, perceived ease of use, perceived usefulness, and system usage.
Karsten et al., 2012	Meta-analysis	102 CSE related articles	Correlates of CSE (computer skill, computer attitude, computer anxiety, perceived ease of use, perceived usefulness, behavioral intention & behavior)	CSE is significantly related to all seven correlates, therefore CSE should be treated as a primary variable of interest in IS research.
Kher et al., 2013		230 university undergraduate students	Questionnaire: Computer anxiety, CSE, and GSCE	Significant increase in CSE observed after about two months of training, non-linear growth trajectory observed for CSE, CSE change strongly predicted by computer anxiety, CSE

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				change significantly predicted software specific CSE.
Laganá et al., 2011	Empirical investigation	96 community-dwelling adults	Survey: Older adults' computer technology attitudes, CUSE, and socio-demographic attributes and computer accessibility/experience	Significant improvements in attitudes and self-efficacy observed because of the training program.
Levy & Danet, 2010	Empirical investigation	217 system users at NASA Langley Research Center	Survey: User involvement, user resistance, CSE, and IS success	CSE and user involvement had positive significant impact on IS success. User's resistance had no significant impact on IS usage. End user involvement had a strong negative impact on user's resistance.
Marakas et al., 1998	Literature review and analysis	40 CSE related studies		Continued research into the methods and measures used in CSE studies was encouraged. There was significant value in the rigorous assessment of the CSE construct at the general and task-specific levels.
Marakas et al., 2007	Empirical investigation	533 university students	Questionnaire: Task performance test, GCSE and specific CSE (Windows, Internet, Database, Word Processing, & Spreadsheet)	CSE was an important variable in IT related studies and could be used to effectively predict end-user performance.

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Phipps et al., 2013	Analysis			Self-efficacy, learning intentions, age, and ability played dominant roles in learning in adults.
Rhee et al., 2009	Empirical investigation	415 graduate business students	Questionnaire: computer experience, security breach incidents, general controllability, self-efficacy in information security (SEIS), security practice - technology, security practice - care behavior, and intention to strengthen the efforts	SEIS positively impacted the use of security software and the security care behavior related to Internet usage; self-efficacy played a dominant role in determining users' InfoSec practices, and served as a motivator in continuously exerting security efforts.
Zhang & Espinoza, 1998	Empirical investigation	220 university students	Survey: CSE, attitudes toward computers, and desirability of learning computing skills.	Participants perceptions of comfort or anxiety about computers predicted their CSE levels; desirability of learning computing skills was predicted by participants' self-recognition of usefulness of computers and their perception of advanced levels of computer technologies.

Older Adults Computer Technology Attitude

According to Abedalaziz, Jamaluddin, and Chin (2013), “an attitude refers to one’s positive or negative judgment about a concrete subject” (p. 201). Within the context of technology usage, attitude refers to an individual’s general assessment or feeling towards specific computer and Internet related activities (Abedalaziz et al., 2013; Smith, Caputi, & Rawstone, 2000). Through experience, attitudes are acquired and, hence, can be modified, i.e. attitudes can change when there is experience or interaction with objects of interests, for example, computers and other associated technologies (Abedalaziz et al., 2013; Czaja & Sharit, 1998; Lagana, 2008; Umemuro & Shirokane, 2003). Similarly, Liaw (2002) related attitude with experience by indicating that the behavioral element of attitude is associated with what an individual will actually do, or intends to do, and that it is affected by the experiences that the individual has.

According to Wagner, Hassanein, and Head (2010), the general belief is that “as age increases, attitudes toward computers tend to become more negative” (p. 872), which would indicate that senior citizens would have negative attitudes towards computers. Due to the pessimistic attitudes of senior citizens towards technology, they were less likely to use the Internet, and as such probably would not try to access it on their own (Iyer & Eastman, 2006). Some of the pessimistic attitudes of senior citizens towards the Internet included a belief that it was dangerous, that they were not missing out on anything by not using it, it was too expensive, and that it was too confusing to use (Iyer & Eastman, 2006). However, Chen and Chan (2013) as well as Schmidt et al. (2014) indicated that contrary to previously held beliefs, senior citizens had an overall positive attitude towards

technology. Research has indicated that the use of various technologies by senior citizens can result in many advantages to them such as allowing them to lead healthier lives, being more socially engaging, and being more independent (Chen & Chan, 2013; Gonzalez, Maria, & Viadel, 2015). More specifically, technologies such as computers, mobile phones, the Internet, and wireless capabilities allow senior citizens to connect remotely with family, friends as well as access services including but not limited to medical, financial, shopping, entertainment, and sports (Chen & Chan, 2013; Wagner et al., 2010). However, although such technologies enhance the aging experience by providing advantages and are supportive to daily living, compared to younger people, senior citizens do not display as much interest in, or attitudes towards using new technologies (Broady, Chan, & Caputi, 2010; Gonzalez et al., 2015). Further, irrespective of how beneficial and how capable technology is, it can only be effectively implemented if users have positive attitudes towards it (Liaw, 2002). After an extensive literature review, Broady et al. (2010) reported that findings from prior research on the technology attitudes of senior citizens and the outcomes of computer training have been contradictory. For example, Ansley and Erber (1988) reported that regarding attitudes towards computers, there were no differences in younger and older users. On the other hand, Laguana and Babcock (1997) as well as Timmermann (1998) reported that senior citizens' experiences with, and attitudes towards computers were negative. Yet still, a general positive attitude towards computers and online usage were reported among senior citizens in other studies (Cody, Dunn, Hoppin, & Wendt, 1999; Eisma et al., 2004; White & Weatherall, 2000). As a result of the senior citizens' positive attitudes towards computers and its influence on online usage, the recommendation was made to include it

in training programmes for senior citizens (Cody et al., 1999; Gonzalez et al., 2015). These evidences from literature indicate mixed and contradictory results regarding older adults' attitudes towards computers. Therefore, since it is still unclear to what extent the computer technology attitudes of senior citizens will influence their technology use, more research in this area is necessary. Further, there have been criticisms about the instrument that has been used to measure computer technology attitudes in senior citizens (Laganá, 2008; Laganá & García, 2013; Laganá et al., 2011). According to Laganá et al. (2011), studies on computer technology attitudes were done on younger populations such as college students, and used instruments such as the Internet Attitude Scale (Zhang, 2007), the Computer Attitude Scale (Loyd & Loyd, 1985), and the Attitudes Toward the Computer Scale (Richter, Naumann, & Groeben, 2000). Jay and Willis (1992) as well as White et al. (2002) conducted attitudinal studies using older populations, however, the same instruments that were used with the younger populations were used. In response, Laganá (2008) developed and validated a 22-item instrument, referred to as older adults' computer technology attitude scale, which was a more appropriate instrument for use with older populations. Since then, Laganá et al. (2011) refined the 22-item older adults' computer technology attitude scale instrument into a validated and reliable 17-item instrument. This study utilized the refined, validated and reliable 17-item instrument in assessing the older adults' computer technology attitude. Consequently, this study added to the body of knowledge in the area of older adults' computer technology attitudes, and specifically investigated if older adults' computer technology attitudes contributed to their motivation to acquire cybersecurity skills.

Table 10

Summary of Older Adults Computer Technology Attitude-related Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Broady et al., 2010	Literature Review			No major differences between attitudes toward computers in older and younger users.
Chen & Chan, 2013	Empirical Investigation	50 adults between 55 and 85 years old	Focus group discussions and interviews: Attitudes toward gerontechnology, reasons for use and non-use of gerontechnology, and facilitators of using gerontechnology	Older people had positive attitudes towards technology. Positive attitudes were related to enhanced convenience and advanced features, e.g. made them feel like they were not obsolete. Negative attitudes were related to health risks and social problems arising from using technology.
Czaja & Sharit, 1998	Empirical Investigation	384 local community participants	Questionnaire: Age, attitude towards computers	Attitudes toward computers can be modified, for example, through direct interaction with new technologies. Positive attitude can increase when there is direct experience with computers, irrespective of age or gender.
Gonzalez et al., 2015	Empirical Investigation	191 seniors between 60 and 89 years old	Questionnaire: Learning about and using computers by	Positive correlation found between senior citizens' attitudes

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			older people, senior citizens' attitudes toward computers, and behavioral patterns of computer use by older people	toward computers and computer use, frequency of Internet access, and self-confidence. Increased positive attitudes resulted from interaction with computers, indicating that attitudes were modifiable.
Iyer & Eastman, 2006	Empirical Investigation	171 senior citizens between 65 and 85 years old	Survey: Attitude towards computers, Internet use, purchase, and comparison shopping	Senior citizens who were most likely to use the Internet, to shop online, and do online comparison shopping were those who had a more positive attitude towards the Internet.
Lagana, 2008	Empirical investigation	32 adults, 65 years or older	Questionnaire and group interview at the end of investigation: CUSE, older adults' attitudes toward computers and the Internet	Developed and validated the 22-item Older Adults' Attitudes toward Computers and the Internet construct. Significant improvement in attitudes toward computers and the Internet resulted from computer and Internet training.
Laganá & García, 2013	Empirical Investigation	60 adults between 51 and 92 years old	Questionnaire: Older adults' computer technology Attitudes, CUSE, self-esteem, and depression	No significant between-group differences in either post-test computer attitudes or self-esteem. Refuted claims that negative computer attitudes

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				in older age can stem from having limited computer technology experience.
Laganá et al., 2011	Empirical Investigation	96 senior citizens	Survey: Older adults' computer technology attitudes, CUSE, and socio-demographic attributes and computer accessibility/experience	Revised and validated the 22-item version of the Older Adults' Computer Technology Attitudes Scale into a shorter 17-item scale. Significant positive attitudes resulted from the training.
Liaw, 2002	Empirical investigation	260 university students	Questionnaire: Computer experience and Web attitude (self-efficacy, enjoyment, usefulness, and intention to use)	Key factors identified for attitudes towards using the Web were computer and Internet experience, motivation, and self-efficacy of individuals.
Umemuro & Shirokane, 2003	Empirical Investigation	16 adults between 60 and 76 years old	Interview and questionnaire: Computer usage, computer attitude, and skill transfer	Experience with computers can change computer attitude. Users with higher computer attitudes were more likely to have higher computer usages.
Wagner et al., 2010	Literature Review	151 articles spanning 1990 to 2008		Existing construct scales that were used to measure computer attitudes in older adults may not be appropriate as they were frequently developed and

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				validated using student samples. Development and validation of more appropriate scales recommended.

Senior Citizens' Use of Computers

Senior citizens make up one of the fastest growing groups of Internet users and evidence has shown that there has been a significant increase in Internet usage among American senior citizens over any other age group in the last decade (Iyer & Eastman, 2006; Perrin & Duggan, 2015; Wagner et al., 2010). For example, senior citizens had a greater rate of increase in Internet usage (107% increase) over all the other surveyed age groups between 2005 and 2015 (Perrin & Duggan, 2015). However, many senior citizens venture into cyberspace without the requisite skills on how to protect themselves against cyber-attacks and that made them very vulnerable to those types of attacks (Grimes et al., 2010). Cyber-criminals often target and exploit senior citizens online, with one in five American senior citizens being a victim of financial fraud, costing more than \$2.6 billion per year (Grimes et al., 2010; Willis, 2015). Jones (2001) indicated that identity theft was one of the common fears of senior citizens when they use the Internet. Additionally, this fear, coupled with their limited cybersecurity awareness and skills, cause them to feel overwhelmed, frustrated as well as demotivated when they use the Internet (Greengard, 2009; Iyer & Eastman, 2006; Jones, 2001).

Using computer technologies including the Internet is required to do everyday tasks such as communicating, shopping, banking, entertainment, and assessing medical information (Slegers et al., 2012; Marquié, Jourdan-Boddaert, & Huet, 2002). Therefore, it is important for senior citizens to possess confidence in their abilities to use the new technologies for these tasks (Marquié et al., 2002). Numerous studies have shown that senior citizens experienced benefits such as increased self-efficacy and improved cognitive functions when they acquired a new skill such as using the computer or the Internet (Gatto & Tak, 2008; Lam & Lee, 2006; Shapira et al., 2007). Shapira et al. (2007) reported that senior citizens viewed using the Internet as an activity of younger persons, therefore, when they realized that they could use it themselves, their self-efficacy was boosted, and they felt as if they were young again. Similarly, Lam and Lee (2006) reported a boost in self-efficacy among senior citizens as they experienced a sense of achievement as well as they were better able to communicate with family and friends via the Internet. However, other studies have identified a lack of self-efficacy as one of the challenges that senior citizens faced, and, thus, prevented them from using new and emerging computer technologies (Kelley & Chames, 1995; Laganá & García, 2013; Marquié et al., 2002). Bandura (1986) had also found that persons who experienced a lack of confidence in their skills would be more reluctant to participate in activities and would abandon the activities when faced with difficulties. Goodwin (2013) indicated that although senior citizens displayed interest in computers and the Internet, they were demotivated to use them because they did not have the requisite skills to complete the required tasks. Since using the Internet has become an everyday activity for senior citizens, there is a need to identify the factors that will motivate them to acquire the

requisite skills so that they will be able to use the new and emerging technologies with confidence (Goodwin, 2013; Grimes et al., 2010; Marquié et al., 2002). It is important to note that while a number of studies have focused on the effects on senior citizens of acquiring skills to use computing technologies such as the Internet, very few have focused on acquiring cybersecurity skills, which would empower them to identify as well as mitigate the evolving problem of cyber-attacks (Grimes et al., 2010; Hart et al., 2008; Lam & Lee, 2006; Ng, 2007). This study filled this gap.

Table 11

Summary of Senior Citizens' Use of Computer-related Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Gatto & Tak, 2008	Descriptive study	58 adults between 59 and 85 years old	Survey: Internet use activities (frequency of during the week, time spent per visit, experience of learning how to use the Internet, types of online activities, Internet use for seeking information, perceived usefulness of online information, barriers & benefits of Internet use)	Older adults experienced both benefits and barriers while using computers. Benefits included utility, satisfaction, a sense of connectedness, and positive learning experiences. Physical and mental limitations, as well as frustration, mistrust, and time issues were listed as barriers.
Goodwin, 2013	Participation action study	10 older adults between 68 and 82 years old	Survey: Computer skill level, comfort	Senior citizens were interested in using the computer; anxiety can be

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			and attitude toward using the computer	decreased and computer confidence improved through personalized training, modifications, and adaptations.
Grimes et al., 2010	Empirical Investigation	Sample 1: 120 participants between 30 and 91 years old. Sample 2: 47 students between 19 and 57 years old	Survey: Computer use, interest, and expertise; privacy and trust; and Internet security awareness	Senior citizens had much lower levels of computer use and Internet security knowledge than younger users.
Iyer & Eastman, 2006	Empirical Investigation	171 senior citizens between 65 and 85 years old	Survey: Attitude towards computers, Internet use, purchase, and comparison shopping	Approximately 50% of participants were dissatisfied with their current Internet skill level; senior citizens who were confident in their ability to use the Internet, comfortable using the Internet, and experienced in using computers were more likely to use the Internet for comparison shopping.
Laganá & García, 2013	Empirical Investigation	60 adults between 51 and 92 years old	Questionnaire: Older adults' computer technology Attitudes, CUSE, self-esteem, and depression	Computer and Internet training resulted in significant improvements in CSE and reduced depression levels in older adults.
Lam & Lee, 2006	Empirical Investigation	939 adults, 55 years or older	Survey and lab experiment: Encouragement	Computer training improved the psychological state of mind and boosted the self-confidence

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
			by others, support, Internet self-efficacy, anxiety, outcome expectations, perceived user competence, and usage intention	of older adults. They will continue computer and Internet usage as they viewed them as tools for learning new topics as well as for communication.
Marquié et al., 2002	Empirical Investigation	91 participants between 24 and 78 years old	Questionnaire: Self-efficacy, computer familiarity, age, capacity, and performance	Older adults did not demonstrate much confidence in their abilities to use new computing technologies. Lack of confidence was a possible challenge that they face in mastering the new technologies.
Shapira et al., 2007	Empirical Investigation	48 older adults between 70 and 93 years old	Questionnaire: Difficulties in physical functioning, life satisfaction, depressive moods, subjective feelings of loneliness, and perceived control	Computer and Internet use by older adults can result in significant improvements such as reduction in depression and loneliness, greater satisfaction with life, enhanced well-being, greater sense of empowerment, and increased cognitive functioning.
Slegers et al., 2012	Empirical Investigation	1256 participants between 24 and 81 years old	Questionnaire: Cognitive abilities, computer and Internet use	Older adults had different predictors of computer use (age, sex, and loneliness) from younger adults (level of education). These predictors needed to be considered when

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
				promoting computer use among older adults.
Wagner et al., 2010	Literature Review	151 articles spanning 1990 - 2008		Computer use by senior citizens is a multi-disciplinary topic; this topic can be broadened and enriched by the different methodologies, constructs, operationalizations, or relationships from other disciplines.

Role of Demographic Variables in Cybersecurity

Several researchers have studied age with gender as demographic variables in research related to cybersecurity threats (Anderson, 2006; Grimes et al., 2010; Purkait et al., 2014; Reisig et al., 2009). Anderson (2006) reported that persons over the age of 75 were less likely to be victims of identity theft and further indicated that the risk that persons in this age group faced was less than half of that which younger persons faced. Reisig et al. (2009) did not find a significant correlation between age and cyber-attacks such as risk of online credit card theft. However, Purkait et al. (2014) and Grimes et al. (2010) reported significant relationship between age and ability to detect cyber-attacks. For example, Grimes et al. (2010) found that older Internet users such as senior citizens were less knowledgeable about cybersecurity threats than their younger counterparts. Similarly, Purkait et al. (2014) found a negative relationship with the Internet user's age

and the ability to detect phishing sites, i.e. as age increased, the ability to detect phishing sites decreased. Regarding gender, Purkait et al. (2014) reported that no significant relationship was found between an Internet user's gender and his/her ability to identify phishing attacks. This was consistent with claims that gender differences should not play a significant role in perceptions of risk towards cyber-attacks (Reisig et al., 2009). Further, Grimes et al. (2010) found that the only time that age was significant in predicting awareness to cyber-attacks was when it interacted with gender; female senior citizens were less knowledgeable about cyber-attacks than younger females, while no significant age difference was found among males. However, Anderson (2006) reported that males were less likely to be victims of identity theft than females. Similarly, Imgraben et al. (2014) found that males were generally more security conscious than females, with males being more restrictive with Wi-Fi connections, read and researched more before downloading apps, and being better at detecting phishing scams. Yet, Lai et al. (2012) reported that males had higher chances of being identity theft victims than females. This was because males used the Internet more, therefore, with this frequent exposure while being on the Internet, they were at greater risks, plus, males had lower perceptions of risks, and hence would not be as careful with protecting their PII (Lai et al., 2012). Hence, these evidences indicate that there is a significant, but contradictory association between gender and cybersecurity threats, and warrants further exploration (Imgraben et al., 2014). Past research had also indicated contradictory results regarding gender and perceived risk (Im, Kim, & Han, 2008; Maddison & Jeske, 2014; Schubert, 2006). For example, Im et al. (2008) found that females perceived lower risks than males in cases prior to embracing technology, and indicated that this finding was dissimilar to

previous studies that indicated that females perceived higher risks than males. On the other hand, Maddison and Jeske (2014) reported that females had a significant higher fear of cyber-victimization than males. Therefore, since it appears that there are contradictory reported results regarding the relationship with age, gender, and cyber-attacks, more research in this area is warranted.

Anderson (2006) indicated that there was no significant relationship between level of education and the probability of being a victim of identity theft. However, according to Grimes et al. (2010), senior citizens who were more educated and have been using the computer for more years were more knowledgeable of, and aware of cyber-attacks. These claims have been supported by later studies by Purkait et al. (2014) and Carlton (2016). Purkait et al. (2014) reported that Internet users who had more years of using the Internet were better able to identify phishing attacks. Similarly, Carlton (2016) found that the number of years of computer use and educational level were significant demographic variables related to the cybersecurity skills level of non-IT professionals. These results suggest that those two variables may help to reduce the number of vulnerabilities and breaches caused by Internet users (Carlton, 2016). Morgan and Ravindran (2014) reported that irrespective of the number of years that senior citizens have been using Internet-enabled mobile devices to access the Internet, in cases where there were high perceptions of risk of cyber-attacks, they would use these devices less to access the Internet. According to Gatto and Tak (2008), senior citizens who had used computers in the workplace prior to retirement brought the computing skills that they learnt into retirement, and were motivated to learn new skills for their personal interests. Additionally, many of those senior citizens who were motivated to learn about the

computers and the Internet would pursue formal computer training sessions or seek assistance from family or friends (Gatto & Tak, 2008). On the other hand, senior citizens who had retired before the ubiquitous use of computers were also less likely to venture into cyberspace because they lacked cybersecurity awareness countermeasures, and were unaware of relevant cyber-attacks, as well as how to mitigate the effects of such attacks (Furnell et al., 2007; Furnell, Tsaganidi, & Phippen, 2008; Grimes et al., 2010). Thus, this study examined the eight aforementioned demographic variables in order to remove any variance that they may have on the effects of the IVs on the DV in the research model (Dinev et al., 2013; Mertler & Vannatta, 2013).

Table 12

Summary of the Role of Demographic Variables in Cybersecurity-related Literature

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contributions
Anderson, 2006	Empirical investigation	>4000 participants	Survey: Age, income, education, number of adults in household, number of children, gender, marital status, race, ethnicity, geographic region, and identity theft	Risk of identity theft declined with age; high risk existed in having more income, one adult in the household, and having more children. No relationship existed with education and marital status.
Grimes et al., 2010	Empirical Investigation	Sample 1: 120 participants between 30 and 91 years old. Sample 2: 47 students between 19 and 57 years old	Survey: Computer use, interest, and expertise; privacy and trust; and Internet security awareness	More educated participants were more knowledgeable about Internet security threats; older participants had lower levels of computer use and Internet security

				knowledge than younger users.
Im et al., 2008	Empirical investigation	161 university students	Questionnaire: Intention to use, perceived risk, perceived ease of use, perceived usefulness, gender, user experience, and technology type	Prior to using technology, females perceived lower risks than males.
Lai et al., 2012	Empirical investigation	117 undergraduate students of a public university in the U.S.	Questionnaire: Identity theft, conventional coping, technological coping, self-efficacy, perceived effectiveness, and social influence	Males had higher chances of being identity theft victims than females due to more frequent exposure on the Internet, plus, they have lower perceptions of risks, and hence would not be as careful with protecting their PII.
Maddison & Jeske, 2014		159 participants	Survey: Perceived likelihood of victimization in the traditional setting, perceived likelihood of victimization in the cyber setting, fear of victimization in the traditional setting, fear of victimization in the cyber setting, self-efficacy, self-esteem, Internet use, and demographic factors (age, gender, & education level)	Females exhibited more fear of victimization in traditional and cyber contexts than males, females had lower self-efficacy than males; the effect of education did not show any significant differences in the fear of cyber-victimization.
Morgan & Ravindran, 2014	Empirical investigation	8130 respondents	Survey: User self-efficacy,	Gender did not significantly affect

			perceived risk, perceived enjoyment, perceived affordability, use of related goods and service, technological consumer good or service (TCGS), perceived ease of use, perceived usefulness, and demographic factors (gender, age, residence, education level, & family income)	Internet or mobile device use; younger users were more engaged in mobile device use than their older counterparts.
Purkait et al., 2014	Empirical investigation	621 Internet users with some experience with online financial transactions	Survey and three experimental tasks: Demographic variables (age, gender, income, education, technical background, family size, & former victim of phishing), awareness on phishing, safe Internet practices, Internet skill, vigilance, memory, and ability to identify phishing website	Gender and educational background did not have significant impacts on the ability of Internet users to correctly identify a phishing website. Age had an inverse relationship with the Internet user's ability to correctly identify a phishing website.
Reisig et al., 2009	Empirical investigation	573 adult Internet users	Telephone interviews and surveys: Perceived risk of Internet theft victimization, behavioral adaptations, financial impulsivity, and	Age did not significantly correlate with risk; females did not display significantly higher risk judgments than males.

sociodemographic
factors (age,
gender, income,
& education)

Summary of What is Known and Unknown in Research Literature

A literature review was conducted and it revealed that HCUs such as senior citizens with access to the Internet are part of the weakest link in InfoSec as the computers that they use are generally not as protected as those used by other younger users or computers in organizations (Kumar, Mohan, & Holowczak, 2008; White, 2015). Cyber-criminals often use the vulnerabilities that exist in HCUs and the computers they use to launch cyber-attacks on the HCUs as well as on other computers that are connected to the Internet (White, 2015). It was also revealed that reports in the literature have placed less attention on investigating cybersecurity awareness issues from the perspective of HCUs, hence the need existed for more research to address these issues and to understand the risks that these users face (Anderson & Agarwal, 2010; Denning, Kohno, & Levy, 2013; White, 2015). Another dearth in the literature existed in using SDT as a theoretical lens in InfoSec behavioral research although it was previously shown to increase users' intrinsic motivation, psychological well-being, persistence and initiative as well as contribute to users' positive behavioral outcomes (Wall et al., 2013). The literature review also revealed that cybersecurity awareness, computer self-efficacy, perceived risk of identity theft, and older adults' computer technology attitudes were factors that can impact the motivation of Internet users such as senior citizens, to acquire cybersecurity skills (Boss et al., 2009; D'Arcy, et al., 2009; Holt & Turner, 2012;

Johnston & Warkentin, 2010; McCrohan et al., 2010). Cybersecurity awareness and skills are required for Internet users to be able to identify and mitigate the effects of cyber-attacks, which in turn, will reduce the significant losses that are caused by such attacks (Abbasi et al., 2010; D'Arcy et al., 2009; Grimes et al., 2010; Shillair et al., 2015). However, acquiring cybersecurity skills requires effort, therefore, Internet users, especially senior citizens, must be motivated before they will expend the necessary effort to acquire such skills (Boss et al., 2009; Shillair et al., 2015). It was also revealed in the literature review that there are contradictory findings on each of the above-mentioned factors, and how each impacted motivation to acquire cybersecurity skills, therefore, this study sheds more light on what motivates Internet users, specifically senior citizens, to acquire cybersecurity skills.

Chapter 3

Methodology

Research Design

This research study used a quantitative research method that utilized a pre-experimental one group pretest-posttest design. A quantitative research method is the best method choice in studies that seek to identify factors that influence an outcome, studies that use a treatment (intervention), and/or in studies that seek to understand the predictors of outcomes (Creswell, 2014). A pre-experimental design is one in which a single group is studied and the researcher provides an intervention during the experiment Creswell (2014). Specifically, the one group pretest-posttest design includes a pre-test measure, followed by a treatment, and then a post-test for a single group (Creswell, 2014). Such was the case in this study as the main goal was to empirically assess the contributions of a single group of senior citizens' SCCA, CSE, PRIT, and OACTA on their motivation (IM & EM) to acquire cybersecurity skills, as well as their CyberSkills level, while comparing before, and after cybersecurity awareness training. There were three phases in this study. In phase one, the survey instrument was developed based on validated measures from prior research, and further validated using an expert-review process that followed the Delphi technique. In phase two, there was a pilot testing of the pre-and-post training measures using the survey instrument and an iPad app, namely MyCyberSkills™ iPad app (Carlton & Levy, 2015; Carlton et al., 2016), for the CyberSkills. The pilot test

further enhanced the validation of the study instrument, and identified potential problems with the study. Phase three was the main data collection of the pre-and-post training measures that addressed the research questions, including data analysis, and interpretation. Since human subjects were used in this study, approval was sought from the IRB before the data was collected. Appendix A shows the IRB approval letter. Figure 2 shows the study’s methodology.

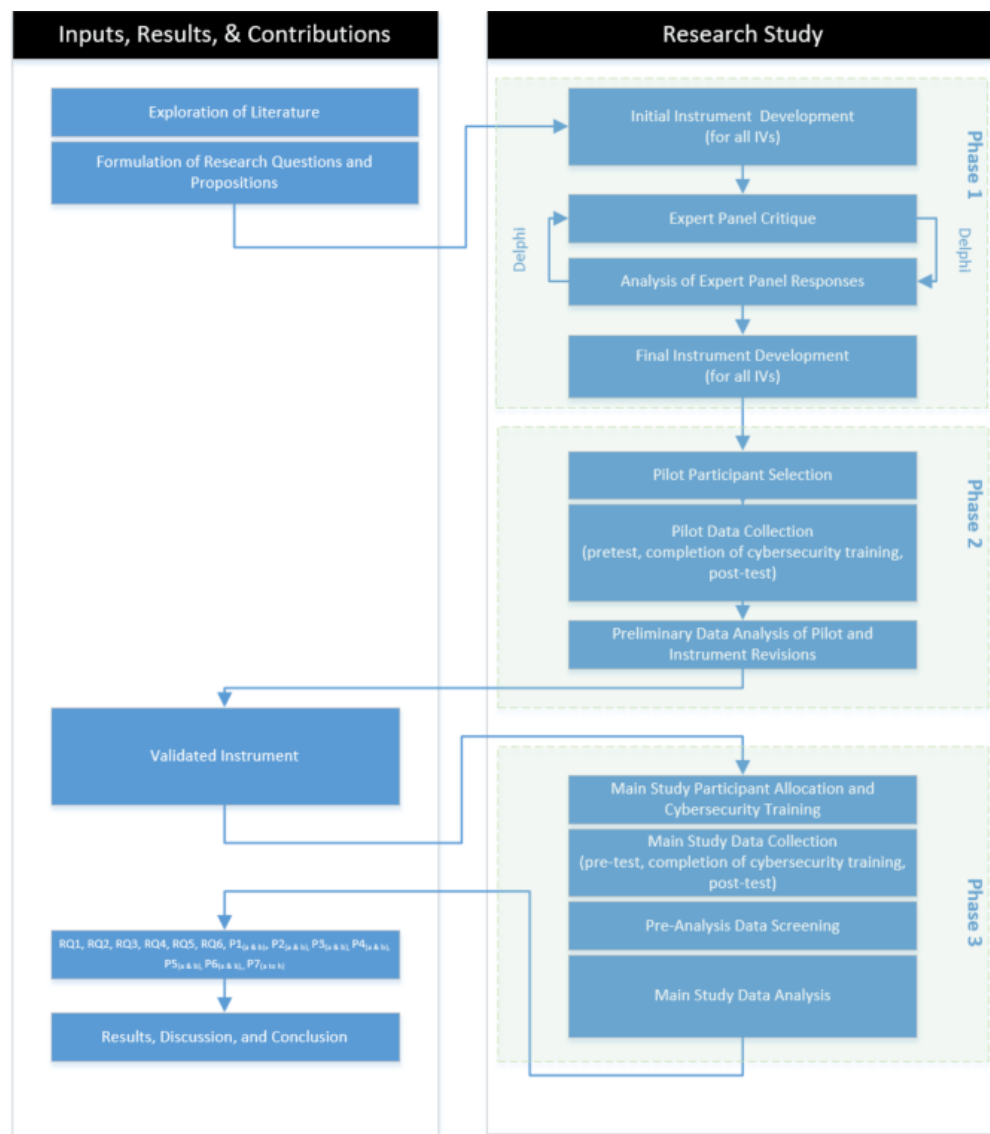


Figure 2. Research Study Methodology

Survey Instrument and Measures

For this study, two survey instruments were initially developed which was then finalized into a single instrument that measured all the identified IVs (SCCA, CSE, PRIT, & OACTA), and the MV (motivation, i.e. IM & EM, to acquire cybersecurity skills). An iPad app was used to measure the DV (CyberSkills), which was previously developed and validated (Carlton, 2017; Carlton & Levy, 2015; Carlton et al., 2015). The survey instrument included six sections for the IVs and the MV, plus the eight demographic control indicators. All the survey items, except for the gender demographic indicator was measured using a 7-point Likert-type scale as using such a scale yields better results because it allows more accurate variability (Cicchetti, Shoinralter, & Tyrer, 1985). As recommended by Straub (1989), all the measures included items from prior research for validity purposes. However, to capture all the constructs, the survey instrument combined items from various studies. Creswell (2014) indicated that when an instrument is modified, or, if different instruments are combined into a single study, the original reliability and validity may not hold true for the new instrument. Therefore, it becomes vital that reliability and validity be re-established during data analysis (Creswell, 2014). Since this study combined instruments from various studies, an expert panel following the Delphi technique, plus a pilot test was done to re-establish reliability and validity of the final instrument. The purpose of the first developed instrument was to get responses from the expert panel, with the aim of assessing the content validity of the identified measures. The responses from the expert panel were used to revise the instrument.

Following the revisions, the second instrument was developed and consequently used in the pilot test to collect the quantitative data on the IVs and MV.

A comprehensive review of the literature for all the constructs being investigated in this study, plus revisions recommended by the expert panel, culminated in the survey instrument shown in Appendix B. The survey instrument included a total of 67 items divided in six sections namely, Cybersecurity Awareness, Computer Self-efficacy, Risk of Identity Theft, Computer Technology Attitude, Interest in Cybersecurity Training, and Demographics. Names of the sections were modified to reduce response bias. Section 1: Cybersecurity Awareness measured how aware senior citizens were of some common cybersecurity threats that they faced when they were online. Six items that were adapted from Kajzer, D'Arcy, Crowell, Striegel, and Bruggen (2014), plus two that were recommended by the expert panel, were used to measure the cybersecurity awareness construct. All six original items were used and were modestly adapted for the context of this study. The literature review for items for the cybersecurity awareness construct revealed that most of the studies on cybersecurity awareness were done within the context of the organization, and assessed employees' awareness level of the organization's security policies, SETA programs, and security countermeasures (Albrechtsen & Hovden, 2010; Bulgurcu, Cavusoglu, & Benbasat, 2010; D'Arcy & Hovav, 2007; D'Arcy & Hovav, 2009; D'Arcy et al., 2009). However, since the focus of this study was on senior citizens who were mostly no longer a part of the workforce, the context of the organization was, thus, outside the study's scope. The focus of this study was on the awareness levels of the senior citizens of cybersecurity threats, hence the items used in the Kajzer et al. (2014) study were most appropriate as they too focused on

specific cybersecurity threats to the individuals. Cybersecurity awareness level was assessed using a 7-point Likert-type scale ranging from “1” to “7”, with “1” indicating “Not at all Aware”, and “7” indicating “Extremely Aware”.

Section 2: Computer Self-Efficacy measured how senior citizens perceive their ability to use the computer. This construct was measured using three items adapted from Compeau and Higgins (1995) as well as Bhatnagar, Madden, and Levy (2016). Bhatnagar et al. (2016) used the three items adapted from the original 10 items from Compeau and Higgins (1995), and found high reliability with a Cronbach’s alpha value of 0.880, which is higher than the acceptable range of at least 0.70 (Hair et al., 2014; Levy & Danet, 2010). All three items were modified to fit the context of this study, and was assessed using a 7-point Likert-type scale ranging from “1” to “7”, with “1” indicating “Strongly Disagree”, and “7” indicating “Strongly Agree”.

Section 3: Risk of Identity Theft measured senior citizens’ belief in the possibility that another individual will unlawfully use their PII for the individual’s personal gain while they, that is, the senior citizens, were online. This study assessed the construct of risk of identity theft using eight dimensions of perceived risk adapted from Zhao et al. (2008). The eight dimensions used a total of 23 items, broken down as follows: performance (three items), security (three items), financial (three items), privacy (three items), time (two items), psychological (three items), social (three items), and physical (two items). All 23 items were modified to fit the context of this study, and was assessed using a 7-point Likert-type scale ranging from “1” to “7”, with “1” indicating “Strongly Disagree”, and “7” indicating “Strongly Agree”.

Section 4: Computer Technology Attitude measured senior citizens' feelings or judgment about computer technology. This construct was measured using 17 items adapted from Laganá et al. (2011). All 17 original items were used and were not modified for this study. Similar to the multi-dimensionality of the Risk of Identity Theft construct, the Computer Technology Attitude construct has four dimensions with corresponding items, namely, comfort communicating via Internet (five items), satisfaction with available computer technology (four items), physical comfort with computer technology (four items), and psychological comfort with computer technology (four items). To get truthful responses from senior citizens who were not familiar with technology, all the items on the instrument were negatively worded, however, during analysis, each item response was interpreted in the reverse (Laganá et al., 2011). The original instrument that was developed by Lagana' (2008) had 22 items which were all used in the Laganá et al. (2011) study. However, after conducting item-analysis and preliminary factor analysis to determine the necessity of keeping each item, Laganá et al. (2011) eliminated five items because of unwanted attributes, redundancy, irrelevance to attitudes toward computers, plus two items were identified as being double-barreled. Additionally, the outcome of the item-total correlations for each of the items showed that those five items were weakly inter-correlated, having an item-total correlation lower than 0.30 (Laganá et al., 2011; Tabachnick & Fidell, 2007). After the five items were eliminated, validity of the overall 17-item scale increased with a very strong Cronbach's Alpha value of 0.92 (Laganá et al., 2011). The 17 items, with modest adaptations for the context of this study, were assessed using a 7-point Likert-type scale ranging from "1" to "7", with "1" indicating "Strongly Disagree", and "7" indicating "Strongly Agree".

Section 5: Interest in Cybersecurity Training measured senior citizens' drive or inspiration to acquire cybersecurity skills. A total of eight items that were adapted from Nausheen (2016) as well as Pintrich, Smith, Garcia, and McKeachie (1993) were used to assess the motivation construct: four items assessed intrinsic motivation, while the remaining four assessed extrinsic motivation. Each item was modified to fit the context of this study and was assessed using a 7-point Likert-type scale ranging from "1" to "7", with "1" indicating "Very Untrue of Me", and "7" indicating "Very True of Me".

Section 6: Demographic Information collected eight demographic indicators from the participants in the survey, namely, (a) age, (b) gender, (c) years of using computers, (d) years of using the Internet, (e) years of using Internet-enabled mobile devices, (f) years of working in corporate or formal organization, (g) years since retiring, and (h) level of education. The rationale for choosing these indicators was previously explained in the literature review in Chapter 2.

Expert Panel

Straub (1989) indicated that it was important to show that instruments that were developed were actually measuring what they were designed to measure and this could be done through literature reviews, pre-testing, and expert panels. As part of validating the content of the survey instrument, this study followed the Delphi technique to elicit responses from an expert panel. Sekaran and Bougie (2013) also recommended the use of an expert panel for content validity of the measures within a survey as an expert panel can attest to, i.e. substantiate, the content validity of the instrument. The Delphi technique is a group communication process that is aimed at achieving an informed judgment with consensus on a particular topic (Ramim & Lichvar, 2014). An expert possesses skills in a

particular field or domain, therefore, in order for the expert panel to perform valid decision making, the participants should be sought based on demonstrated competencies that are related to the assessment of the decision making (Gabel & Shipan, 2004; Carlton & Levy, 2015; Mattord, Levy, & Furnell, 2013). As such, a group of 30 expert panel participants consisting of IS faculty members, IS doctoral students, and IS professionals in various industries were selected for this study. The members of the expert panel were recruited via email messages on LinkedIn and directly to doctoral students as well as other IS professionals. Appendix C shows the expert panel recruitment email letter. The expert panel validated the questions to determine if the selected survey items met the requirements in terms of understandability, answerability, and readability (Ramim & Lichvar, 2014). The literature recommends that the feedback that is received during each round of the Delphi technique should be used to encourage the expert panel to review their initial responses until a consensus is met (Okoli & Pawlowski, 2004; Ramim & Lichvar, 2014). Since there was consensus amongst the experts during the first round of this study, it was not necessary to include other rounds. Appendix D provides the quantitative and qualitative instrument for the expert panel.

Pilot Test

After the consensus and adjustments were made following the feedback from the expert panel, and prior to the main data collection, the final survey instrument, along with the MyCyberSkills™ iPad app was used in a pilot test to examine their usability. A pilot test is a trial before the main study is done, therefore, it administers the exact procedures that will be used in the main study to a small group of participants similar to those who will be used in the main study, and is very useful in refining the survey questions (Dane,

2011; Zikmund, 2013). A pilot test can further enhance the content validity of a survey instrument as well as help to improve the questions, their format, and the scales that are used (Creswell, 2014; Rea & Parker, 2014). This study used 27 participants who were similar to the characteristics of the main study participants to take part in the pilot test. Appendix E provides the pilot test participant recruitment email letter. Feedback from the pilot test was used to finalize the survey instrument. Additionally, other problems that were encountered during the pilot test were addressed prior to the main study. Appendix F provides the quantitative and qualitative instrument to the pilot test participants.

MyCyberSkills™ iPad app

Instruments that measure skills have been a challenge in the IS domain, as in most cases, self-reported survey instruments were used, and they measured a user's perceptions of his or her skills, rather than his or her actual skills (Carlton & Levy, 2015; Levy, 2005; Torkzadeh & Lee, 2003). Torkzadeh and Lee (2003) cautioned that the results from such instruments can be misleading as users may inaccurately report their skills since "perceptions do not always correspond to reality" (p. 612). Weigel and Hazen (2014) posited that both perceived skills and actual skills should be considered when measuring IT skills, as this would give a more comprehensive picture of a user's skills level. White (2015) also echoed this argument by calling for future research that measured actual security incidents and computer activity of users instead of reporting from memory. Similarly, other researchers have called for further research into assessing the actual security actions of Internet users, rather than their security intentions, in order to enhance the understanding of what motivates the users to protect themselves from cyber-attacks (Boss, Galletta, Benjamin Lowry, Moody, & Polak, 2015; Tsai, Jiang,

Alhabash, LaRose, Rifon, & Cotten, 2016). Carlton (2016) and Choi (2013) emphasized that there was a dearth in the literature regarding instruments to measure actual cybersecurity skills, plus the few that were found were dated and limited. Hence the need existed to develop a measure that was based on scenarios that emulated real-life cases of cyber-attacks (Carlton, 2016). In response to this, Carlton (2016) developed a scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills that was operationalized into an app, namely, MyCyberSkills™ iPad app. Weigel and Hazen (2014) had indicated that due to the rapid changes in technology, measures and constructs that relied on interaction with specific technologies would need to be continuously updated to stay relevant. To address this issue, the scenarios in the MyCyberSkills™ iPad app represented real-life cases of cyber-attacks and were platform independent, that is, they were not tied to a specific platform and/or operating system (Carlton, 2016). The MyCyberSkills™ iPad app was empirically tested and validated following a rigorous research methodology (Carlton, 2016).

Therefore, the CyberSkills construct in this study was measured using the MyCyberSkills™ iPad app, and was adapted without modification. Carlton and Levy (2015) had identified the top nine cybersecurity skills that were needed by non-IT professionals to counter cyber-attacks. The identified skills were (1) preventing the leaking of confidential digital information to unauthorized individuals, (2) preventing malware via non-secure Websites, (3) preventing personally identifiable information (PII) theft via access to non-secure networks, (4) preventing PII theft via e-mail phishing, (5) preventing malware via e-mail, (6) preventing credit card information theft by purchasing from non-secured Websites, (7) preventing information system compromise via USB or

storage drive/device exploitations, (8) preventing unauthorized information system access via password exploitations, and (9) preventing PII theft via social networks (Carlton & Levy, 2015). The MyCyberSkills™ is comprised of a set of hands-on tasks that were used to measure the user's actual cybersecurity skills. According to Carlton (2016), each of the nine skills is assessed via four cybersecurity related hands-on tasks, and the senior citizen was asked to make decisions on specific real-life situations and demonstrate his/her skill level. Each cybersecurity related task was presented individually, and begun with a scenario. After the first task was completed, the second scenario was presented to start task two, and this continued until all four tasks for a particular skill were completed. Each task within the skill incremented in difficulty level and had four response options from which to choose. For each response that the senior citizen selected, the app recorded the performance level using a scale of zero to 10, prior to presenting the next task. Within each skill, the difficulty level ranged from (a) easy to (b) somewhat difficult, to (c) difficult, and then (d) very difficult. Using an interval of zero to 40, a total weighted score was possible for each cybersecurity skill. When all the tasks were completed, the app displayed the overall score interval of zero to 100 and the score interval of zero to 100 for each individual cybersecurity skill that was achieved by the senior citizen. The overall score was then used as the DV in the model.

Instrument Validity and Reliability

A valid instrument is one that actually measures what needs to be measured, while a reliable instrument is one that measures the same thing more than once and produces the same outcomes (Salkind, 2012). According to Creswell (2002), the reliability and validity of an instrument should provide “an accurate assessment of the variable and

enable the researcher to draw inferences to a sample or population” (p. 180). As such, Salkind (2012) further stated that validity and reliability were the first line of defense that a researcher had against making erroneous conclusions. In fact, “if the instrument fails, then everything else down the line fails as well” (Salkind, 2012, p. 115). Straub (1989) indicated that it was important to show that instruments that were developed were actually measuring what they were designed to measure. The importance of instrument validation had also been emphasized in subsequent studies which indicated that in the absence of instrument validation, the findings and interpretations of studies lacked rigor, as well as were not trustworthy (Boudreau, Gefen, & Straub, 2001; Straub, Boudreau, & Gefen, 2004). Straub (1989) indicated that pilot tests can be used to measure reliability and construct validity, therefore, this study used a pilot test to minimize the threats to reliability and validity of the survey instrument. Two types of validation that can be used for the trustworthiness of research results are content validation and construct validation (Salkind, 2012; Straub, 1989).

An “instrument valid in content is one that has drawn representative questions from a universal pool” (Straub, 1989, p. 150). Further, Creswell (2002) stated that “content validity is the extent to which the questions on the instrument and the scores from the questions are representative of all the possible questions that could be asked about the content or skills” (p. 184). On the other hand, construct validity refers to “a determination of the significance, meaning, purpose, and use of scores from an instrument” (Creswell, 2002, p. 184). It focuses on “whether the scores serve a useful purpose and have positive consequences when they are used in practice” (Creswell, 2014, p. 159). Content validity can be established through literature reviews, an expert panel,

and pilot tests (Boudreau et al., 2001, Creswell, 2002; Straub, 1989). This study used all three recommended techniques to establish both content and construct validity.

Internal Validity

According to Leedy and Ormrod (2005), internal validity of a research study is the “extent to which its design and the data that it yields allow the researcher to draw accurate conclusions about cause-and-effect and other relationships within the data” (p. 103-104). Internal validity can refer to both the instrument used and the design of the study (Creswell, 2012; Sekaran & Bougie, 2013). Threats to internal validity regarding the survey instrument have been previously addressed. Internal validity regarding the design of the study includes seven types, namely, history, maturation, regression, selection, mortality, testing, and instrumentation (Creswell, 2012; Sekaran & Bougie, 2013). The first five relate to the participants in the study, while the latter two relate to the procedures of the study (Creswell, 2012). History and maturation threats involve uncontrollable changes during the length of the study that could influence the outcome, such as the study being conducted over a long period of time and the participants may mature or change over the period of the study (Creswell, 2012). This study addressed these threats by conducting the study over a short period of two to four weeks, and used participants who matured at the same rate, that is, senior citizens who were in the same age range. Regression and selection threats involve researcher bias for the selection of the participant and can influence the outcome (Creswell, 2012; Sekaran & Bougie, 2013). Random selection of participants has been recommended to increase internal validity (Creswell, 2012; Sekaran & Bougie, 2013). Therefore, this study randomly selected participants who met the specified criteria for the study. Mortality refers to attrition rate

or the possibility of participants dropping out over the period of the study (Creswell, 2012; Sekaran & Bougie, 2013). Mortality was a threat to this study in two ways: experts from the expert panel could drop out during the Delphi technique process, and senior citizens, who could drop out of the study for any number of reasons. Since this study did not expect that 100% participation would be maintained over the period of the study, in order to account for mortality, at least 30 experts and over 500 senior citizen participants were initially invited (Creswell, 2012; Sekaran & Bougie, 2013). Additionally, gifts or 'in kind' rewards may also be given to participants to encourage participation (Scheele, 1975). This study provided refreshments and a social interaction environment for the seniors during and after the training sessions. Testing refers to when participants are exposed to a pre-test that can influence a post-test, in that the participants would become familiar with the outcome measures during the pre-test, and remember the responses for the post-test (Creswell, 2012; Sekaran & Bougie, 2013). This study used a pre-test and post-test, therefore testing was a threat. To mitigate this threat, the post-test was only administered once (Creswell, 2012). Additionally, Greengard (2009) stated that senior citizens face cognitive challenges such as fading memory and slower speed at processing information, therefore, they were not expected to remember the responses for the post-test in this study. Also, the post-test was given at least one week later, and this made it more difficult for the participants to remember their previous answers. Instrumentation threats refers to a change in the measuring instrument between pre-test and post-test, however, this threat can be mitigated by standardizing the procedures so that the same scales or instrument are used for both pre-test and post-test (Creswell, 2012; Sekaran &

Bougie, 2013). This study used the same measuring instruments throughout the entire period of the study.

External Validity

The extent to which the results of a study and conclusions made can be generalized to other settings, people, or events is referred to as external validity (Ellis & Levy, 2009; Leedy & Ormrod, 2005; Sekaran & Bougie, 2013). It is important that researchers demonstrate that the results of the research are applicable to natural, that is, non-contrived settings, rather than artificial, that is, contrived settings, for example a laboratory (Ellis & Levy, 2009; Sekaran & Bougie, 2013). Three key points to note when addressing external validity are to have a sample that is representative of the population on which the researcher intends to draw the conclusions on, having an adequate sample size, and where the study is conducted (Leedy & Ormrod, 2005). The larger the sample size, the more generalizable the research results will be (Leedy & Ormrod, 2005). To demonstrate external validity, this study reached out to approximately 500 senior citizen participants, and was conducted outside of a laboratory. Additionally, eight demographic indicators were collected to ensure that the data collected is a good representative of the sample and population that the conclusions were drawn on (Compeau, Marcolin, Kelley, & Higgins, 2012).

Specific Research Steps

After participants were recruited and acceptance to participate was obtained from each, they were asked to attend a "lab session" where each was given a random UserID on a printed card (e.g. "C1019"). Specific instructions about the research was given,

followed by the link to the online survey (pre-test) that measured all the IVs and MV. The instructions included highlighting the importance of entering the UserID in both the survey and the skills assessment tool. The UserID was used to ensure that the scoring from the MyCyberSkills™ iPad app, the DV, could be matched to the survey scoring of each participant in an anonymized form. The UserID was a required field on both the survey and the skills assessment, therefore, each participant was required to enter the assigned UserID in the online survey and the MyCyberSkills™ iPad app. In the survey, each was asked a set of questions for each IV/MV, including some demographic information, and each was required to enter his/her anonymous responses to all questions via the computer. Participants could only make one selection per question and all questions had to be answered before the survey could be submitted to avoid missing data. No PII were collected. After completing and submitting the survey, a pop-up acknowledgement window appeared which also contained the clickable link to the MyCyberSkills™ app for participants to take the cybersecurity skills assessment (also a part of the pre-test). The app also collected some demographic information from each participant before beginning the assessment. In the assessment, a total of nine cybersecurity skills were measured, and each skill had four associated tasks. A short story/scenario begun each task, and participants had the option to read or listen to the scenario via earbuds or headphones. At the end of each scenario, participants were asked to choose how the person in the scenario should respond to the situation. This process continued until all the scenarios, tasks, and skills were completed. At the end of the assessment, participants were provided with the score for each skill as well as with an overall cybersecurity skills index score from zero to 100. The survey responses and

corresponding scores from the cybersecurity skills assessment were anonymously recorded and stored via a Google spreadsheet. These represented the pre-test measures. Both the survey and the assessment took about 90 minutes an average to complete, after which participants were required to leave the “lab session”.

After about one week, participants were asked to attend another “lab session” to receive cybersecurity awareness training. The training content included, but was not limited to content that related to the nine cybersecurity skills that were needed by non-IT professionals as identified in the Carlton and Levy (2015) study. Some of the topics that were covered were preventing the leaking of confidential digital information to unauthorized individuals, preventing malware via non-secure Websites, preventing PII theft via access to non-secure networks, preventing PII theft via e-mail phishing, preventing malware via e-mail, preventing credit card information theft by purchasing from non-secured Websites, preventing information system compromise via USB or storage drive/device exploitations, preventing unauthorized information system access via password exploitations, and preventing PII theft via social networks. The training was delivered using a combination of videos, PowerPoint presentation, and instructor-led explanations. After the training, participants were given the links to the same online survey and MyCyberSkills™ app, and they were asked to enter their responses to the survey items, and also re-take the cybersecurity skills assessment. The same UserID that each participant was assigned before, was used in the survey and skill assessment tool. The responses and corresponding scores from the assessment and survey instrument were recorded and stored in the Google spreadsheet. These represented the post-test measures.

The training, survey, and assessment took about three to four hours to complete.

Participant were then required to leave the “lab session” and the data collection ended.

Population and Sample

This study included a sample of 254 senior citizens. To be selected to participate in this study, senior citizens had to be 60 years or older and had been accessing the Internet via an Internet-enabled mobile device such as a mobile phone, tablet/iPad, or laptop computer for at least one year. Age was part of the demographic data that was collected from the participants to ensure only senior citizens participate in the study. Other anonymous demographic data that were collected included gender, years of using computers, years of using the Internet, years of working in corporate or formal organization, years since retiring, and level of education. According to Terrell (2012), collecting this type of data will assist in identifying the characteristics of the participants. In order to reach to participants in senior citizens communities, the sample was collected in smaller groups also to allow for the delivery of the cybersecurity training. The group size ranged from nine to 30 participants and the cybersecurity awareness training lasted for about two hours. Participants were recruited via email inviting them to participate in the study. Appendix G provides the participant recruitment email.

Pre-Analysis Data Screening

Levy (2006) as well as Mertler and Vannatta (2013) have emphasized the importance of pre-analysis data screening to ensure accuracy of the collected data before statistical analysis is done. Mertler and Vannatta (2013) further pointed out that

inaccurate data in research will have direct impacts on the validity of the results and the ability to draw valid conclusions from the collected data. “Pre-analysis data preparation deals with the process of detecting irregularities or problems with the collected data” (Levy, 2006, p. 150). The primary purposes of pre-analysis data screening are four-fold: to ensure that the data is accurate, to take care of missing data, to handle response-set issues, and to deal with extreme cases, i.e. outliers (Levy, 2006). In this study, a Web-based survey was used to collect data from the expert panel, pilot test participants, and the main participants (pre-&-post-test measurements), along with the automatic recording of the cybersecurity skills scores on the MyCyberSkills™ iPad app. A major advantage of using Web-based surveys is that since the computer captures the responses, they allow full automation of data entry into analysis programs, which minimizes data entry or transcription errors (Creswell, 2012; Fan & Yang, 2010). Therefore, the Web-based survey facilitated the accuracy of the collected data as it had some automatic capabilities, including a standard set of responses, mostly using a 7-point Likert-type scale, with each question marked as required. The Statistical Package for the Social Sciences (SPSS®) also helped to facilitate data accuracy by further examining the data for frequency distributions and descriptive statistics (Mertler & Vannatta, 2013).

Specifically, to address each of the four-fold purpose of pre-analysis data screening, the following steps were done. Errors that can arise from transcribing data was eliminated with the use of automatic capturing of the item responses on the Web-based survey, and the automatic recording as well as tabulation of the cybersecurity skills score within the MyCyberSkills™ iPad app. Each question on the Web-based survey was marked as a required question, and the survey could not be submitted until all the

questions were answered. This eliminated any instance of missing data. It is important that instances of missing data be mitigated as missing data can significantly affect the validity of the collected data, the conclusions that are drawn from the data, and the ability to generalize the results to a broader population (Levy, 2006; Mertler & Vannatta, 2013). The data was also reviewed for instances of response set. According to Levy (2006), response set occurs when participants in a survey select the same score for all the survey items, and this can negatively affect the validity of the results. All identified instances of response set were further examined and was considered for elimination from the analysis. Extreme cases or outliers are instances where extreme or unusual scores are found at either or both ends of a sample distribution, and can distort the results of the data analysis (Levy, 2006; Mertler & Vannatta, 2013). Outliers can be detected by Mahalanobis Distance procedure (Mertler & Vannatta, 2013). This study used Mahalanobis Distance procedure to detect outliers, and any identified instances were considered for elimination from the data analysis.

Data Analysis

To address the research questions and propositions, this study utilized several statistical analyzes, including data aggregation, and the tabulation of the scores from the MyCyberSkills™ iPad app. The relationships among the IVs and DV were assessed using path analysis in Partial Least Square - Structural Equations Modeling (PLS-SEM). Widely used in IS research, PLS-SEM is used when the research objective is prediction and explanation of target constructs (Gefen & Straub, 2005; Hair, Hult, Ringle, & Sarstedt, 2014; Levy & Danet, 2010). Gefen, Straub, and Boudreau (2000) also indicated

that PLS is the technique of choice for predictive applications and theory building as it is designed to explain variance, i.e. to assess the significance of relationships and their resulting coefficients of determination or R-squared (R^2). The path in analyzing the data included examining the relationship between SCCA, CSE, PRIT, and OACTA (IVs), their impact on motivation (IM & EM) to acquire cybersecurity skills, and its impact on CyberSkills level (as the DV). The contributions of the IVs on the DV in the path relationship were assessed. Path analysis in PLS-SEM, therefore, addressed RQ1 to RQ4, as well as P1 to P5. Analysis of variance (ANOVA) was used to determine if there were significant mean difference between the pre-and post-test levels of the DV in the senior citizens. This addressed RQ5 as well as P6. ANOVA is used to test “the significance of group differences between two or more means as it analyzes variation between and within each group” (Mertler & Vannatta, 2013, p. 15). Within the context of this study, there were pre-and post-test measurements of the DV, therefore, ANOVA was used to test if there were significant mean difference between the two sets of measurements. Analysis of covariance (ANCOVA) was used to determine if there were significant mean difference between the pre-and post-test levels of the DV, when controlled for the demographic indicators. This addressed RQ6 and P7. ANCOVA is used to examine group differences when controlling for covariates, which, ultimately will give a clearer picture of the true effects of the IVs on the DVs (Mertler & Vannatta, 2013). Control variables have been included in studies when other factors than those included in the research model have a potential influence on the model (Dinev, Xu, Smith, & Hart, 2013). The control variables are included to remove the variance explained by them, and hence, give stronger indications of the effects of the IVs on the DVs in the model (Dinev

et al., 2013; Mertler & Vannatta, 2013). This is appropriate for this study as it controlled for eight demographic indicators, namely: (a) age, (b) gender, (c) years of using computers, (d) years of using the Internet, (e) years of using Internet-enabled mobile devices, (f) years of working in corporate or formal organization, (g) years since retiring, and (h) level of education.

Data Aggregation

Since the perceived risk of identity theft construct was assessed as a multi-dimensional construct, data aggregation was necessary to calculate the overall perceived risk of identity theft. Using the additive model, Dowling (1986) calculated overall perceived risk as the summation of the user assessed perceived risk values for the dimensions that have been selected to be studied. As previously mentioned, this study used those same eight perceived risk dimensions, namely performance, financial, social, psychological, security, privacy, physical, and time. Therefore, this study summed up all the scores of the user perceived risk dimensions to calculate the overall perceived risk of identity theft score, which was then used in the data analysis. Similarly, the cybersecurity skills score that was used in this study is an aggregation of the nine skills that were accessed (Carlton & Levy, 2015). The MyCyberSkills™ iPad app automatically aggregated the various skill scores and calculated the overall cybersecurity skills score for each participant.

Resources

This study needed the following resources: IRB approval because human subjects were used; access to cybersecurity experts for the expert panel; access to senior citizens,

and access to computer with the following software: Word, Excel, PowerPoint, Visio, SPSS[®], and Smart PLS 3.0. The software was used for writing the dissertation report, creating the training presentation material, and for doing the various statistical analyses.

Summary

The methodology for this study is presented in Chapter 3, and as discussed, a quantitative research method utilizing a pre-experimental one group pretest-post-test design was employed. The study had three phases. Instrument development and validation was done in phase one, which included using an expert panel following the Delphi Technique to validate the items that were drawn from literature (Ramim & Lichvar, 2014; Sekaran & Bougie, 2013; Straub, 1989). A pilot test to further validate the instrument and identify problems that could arise in the main study was done in phase two (Creswell, 2014; Dane, 2011; Rea & Parker, 2014; Zikmund, 2013). Phase three was the main data collection with interpretation and analyses. The specific steps in the study, population and sample, pre-analysis data screening, as well as data analysis were also discussed. Several statistical analyses were done to answer the research questions, such as path analysis in PLS, as well as group differences in ANOVA, and ANCOVA. The chapter concluded with the resources that were needed to conduct the study.

Chapter 4

Results

Overview

This chapter outlines the techniques used to conduct the data analyses and presents the results of such analyses for this study. As previously mentioned, there were three phases to this study, and the results are presented in the order in which each phase was conducted. The survey instrument was developed based on validated measures from prior research, and further validated using an expert-review process following the Delphi technique in phase one. Pilot testing of the pre-and-post training measures using the Web-based survey instrument and an iPad app, namely MyCyberSkills™ was conducted in phase two. The main data collection of the pre-and-post training measures that addressed the research questions, including data analysis, and interpretation was done in phase three.

Phase One - Validation Procedures for Survey Instrument

Straub (1989) recommended that for validity purposes, all measures should include items from prior research. Further, Creswell (2014) indicated that instrument validity and reliability be re-established if the instrument is modified, or, if different instruments are combined into a single study. As previously mentioned, this study combined instruments from various studies, therefore, an expert review process,

following the Delphi technique was used to re-establish reliability and validity of the survey instrument.

Expert Panel

Direct emails and messages via LinkedIn were sent to 30 IS experts soliciting participation on the expert panel to further validate the survey instrument. The 30 experts included IS faculty members, IS doctoral students, as well as IS and InfoSec professionals in various industries. Of the 30 who were contacted, 20 responded, with a response rate of 66.6%. The link to a Web-based survey that included screenshots of the draft survey instrument was sent to the experts and they provided feedback via qualitative sections on the survey. Recommendations included the following:

- The removal of the definition for each construct as it made the survey too long
- The addition of the text “How aware are you of...” to each SCCA item as it would be easier for the senior citizens to remember, rather than placing it once at the top of that section
- The addition of social engineering and ransomware attacks to the SCCA items as these have become prevalent and are very relevant to senior citizens
- Other minor modifications to the layout of the survey instrument, plus modifications to some of the survey items to make them more specific to senior citizens, and also to improve clarity

Overall, the experts' feedback was positive and, based on the recommendations, revisions were made to the survey instrument to finalize it into the final instrument that was approved by expert consensus. This was the instrument that was used in the pilot test.

Phase Two - Pilot Test

Subsequent to the revisions to the survey instrument based on the feedback from the expert panel, a pilot test was conducted using the modified survey instrument, to further improve validity. The pilot test participants were representative of the target demographic population, that is, senior citizens, 60 years or older who have been accessing the Internet for at least one year. Emails soliciting participation were directly sent to seniors and an information session was held with approximately 50 seniors. There were 27 seniors who responded with a response rate of 45.7%. Feedback from the pilot study participants did not result in any changes to the survey instrument, indicating that the questions, their format, and the scales that were used were appropriate for this study, and hence provided content validity. However, based on the feedback, changes were made to how the data collection was done, as some potential problems were identified. It was recommended that since the participants were Internet users who were already familiar with technology, they should be given the option to complete the pre-test on their own time, rather than making it a requirement to come to a computer lab to complete it. Additionally, it was also recommended that since the participants were exhausted after the 2-hr training session, that all participants be asked to complete the post-test outside of the computer lab, however, up to a day following the training. These modifications were

well received by the participants, especially since it would limit the number of times for the participants to physically come to the computer lab. As a result of these recommendations, the main data collection phase was modified and conducted in the manner as outlined in the Main Data Collection Procedures section below.

Phase Three - Main Data Collection

Main Data Collection Procedures

Emails with an attached flyer with information about the study were sent to the heads (e.g. Executive Director) of various organizations that had connections with senior citizens, soliciting their help with recruiting participants. The heads would then send an email blast with the flyer asking interested senior citizens to inform on their willingness to participate. Initially, approximately 350 seniors responded expressing an interest to participate. All interested participants were then emailed a document that specifically outlined the research objectives, participation requirements, participation steps, how the research would be conducted, options to participate (i.e. completing the pre-test at home or come to a computer lab), IRB rights, dates/times/locations for the cybersecurity awareness training sessions as well as deadlines to complete the pre-and-post-tests. The inclusion of options to participate was one of the changes that was implemented as a result of feedback from the pilot test. Acceptance to participate was indicated by participants responding with their options to participate and the date/time/location that they could attend the training. Acceptance emails were received from approximately 335 seniors. Valid participation involved full completion of three parts: Part one included completing the pre-test, i.e. the online survey and the online cybersecurity skills

assessment – participants could choose to do Part one at home or in a computer lab. Part two included mandatory attendance to a 2-hour cybersecurity awareness training session. Part three included completing the post-test, i.e. the same online survey and the same online cybersecurity skills assessment. The links to both were emailed to all participants for them to complete at home, instead of completing in the computer lab as it would have been too tiring for the participants to complete after the training. This was another of the changes that was implemented as a result of feedback from the pilot test.

In Part one, participants who opted to do the pre-test at home were provided a unique random and anonymous UserID#, specific instructions, and the links to both the survey and the cybersecurity skills assessment, along with a due date for completion. Part one had to be completed prior to attending the training, i.e. Part two. Participants who opted to come to the computer lab were given their UserID# on a printed card upon arrival, then they were randomly placed at computer stations that already had the links opened. Specific instructions were then given on completing both the survey and skills assessment. It was also communicated to the participants in attendance that assistance would not be given regarding offering explanations on choosing the correct responses. Rather, assistance would only be given if they were of a technical nature, e.g. server connection problems. Those who opted to come to the computer lab stated that although they had computers at home, they came to the computer lab because they felt more comfortable knowing that assistance was provided in case needed. The specific instructions (for both those who completed at home & those who came to the computer lab) included highlighting the importance of entering the same UserID # in both the survey and the skills assessment tool. The UserID # was used to ensure that the scoring

from the MyCyberSkills™ iPad app could be matched to the survey responses of each participant in an anonymized form, no recording or tracking of which participant got any of the randomized/anonymous UserID # was done to ensure IRB compliance. Participants could only make one selection per question and all questions had to be answered before the survey could be submitted. No PII were collected. After completing and submitting the survey, a pop-up acknowledgement window appeared which also contained the clickable link to the MyCyberSkills™ app for participants to take the cybersecurity skills assessment. At the end of the assessment, the app automatically generated the overall cybersecurity skills index score from zero to 100 for each participant. Participants were encouraged to make a note of the pre-test scores so that they could compare with the post-test score on their own. Most used their phone cameras to take a screen shot of the displayed results. The survey responses and corresponding scores from the cybersecurity skills assessment were recorded and stored via separate Google Forms spreadsheet. Participants who opted to do the pre-test in the lab could leave after they completed the pre-test.

A couple days after completing Part one, emails were sent to all the participants with reminders about attendance to the training (Part two) as well as to encourage completion of Part one prior to attendance (for those who opted to do Part one at home). On average, training sessions were held approximately one week after completing Part one. For Part two, most training sessions were conducted in a computer lab setting although the participants did not use the computers during the sessions, while others were conducted in generic training rooms that had a multi-media projector and screen. Upon arrival at the computer lab, all participants were greeted and then given printed handouts

of the presentation material that they could make extra notes on during the session. Refreshments were available at each session and participants enjoyed the social interaction before, during, and after the sessions. Some also shared their pre-test scores with others and spoke about challenges they had completing Part one. It could be observed that most were happy, or at least relieved, that the challenges were similar amongst all. The sessions were very interactive and covered the nine cybersecurity skills that were identified as needed by non-IT professionals in the Carlton and Levy (2015) study as previously mentioned in Chapter 3. Each session lasted for approximately two hours and was conducted in basically the same manner: first each of the nine cybersecurity threats (for which each skill was required) was defined, with examples, followed by ways to identify each threat, and finally, countermeasure strategies to protect or mitigate against the threats when they arise, i.e. what to do when faced with the threats or, skill required to counter the threat. Along with instructor-led explanations, videos and demonstrations were used to augment the explanation of each topic. For example, a fake Wi-Fi connection was set up to demonstrate how easy it was to connect to free/public Wi-Fi connections when Wi-Fi is enabled on a mobile device, along with the dangers of using free/public Wi-Fi connections. It was also demonstrated how to disable Wi-Fi and Location on mobile devices, how to hover the mouse over links to detect fake Websites in phishing emails, etc. Lively interactive question and answer section would follow each presentation. Even after the session ended, some seniors would remain to ask additional questions.

After each session, all participants who attended the training were sent “Thank You” emails along with the electronic version of the training content that included links

to the videos that they could always refer to in the future. Another email was also sent with instructions, the post-test links to the same online survey and same cybersecurity skills assessment, as well as a due date for completion. Participants were also encouraged to review the presentation material prior to completing the post-test. Results of the survey and skills assessment responses were again captured in separate Google Forms spreadsheets for post-test.

The main data collection period lasted for about three months, i.e. from January to March, 2018. It should be noted that during the first month or so of the data collection period, there were connection and time-out issues with the sever that hosted the MyCyberSkills™ app resulting in the screens freezing very frequently. Numerous telephone calls and emails were received from participants who expressed frustration at the problems they were having – some even stated that they felt that they were the ones causing the problems because they were not following the instructions. A few of them eventually gave up and did not complete the post-test, even after attending the training. The MyCyberSkills™ app was eventually moved to another server, which solved the connection and time-out issues.

Pre-Analysis Data Screening

After the data collection period ended, and prior to data analysis, pre-analysis data screening was conducted to ensure data accuracy (Levy, 2006). The responses from the pre-and-post-tests for both the survey and cybersecurity skills assessment were downloaded from the Google Form spreadsheets into Microsoft Excel where they were sorted by the anonymous UserID # and then by date of completion. Each valid participation required two sets of responses, plus attendance to the training: one set for

the pre-test, i.e. survey and skills assessment, plus another for the post-test. It was revealed that of the 335 participants who indicated acceptance, 81 did not complete all three parts, hence, usable responses from 254 participants remained. The data was visually inspected for response-set issues where participants selected the same answer for all the questions, and no significant response-set issues were identified. The data was then loaded into SPSS® to continue pre-analysis data screening. Descriptive statistics were used to identify missing values, means, standard deviations as well as minimum and maximum values. All the questions on the survey and the cybersecurity skills assessment were marked as required to eliminate missing data, plus participants had to choose from a standard set of responses. The descriptive statistics confirmed that there were no missing values, all responses were within the specified ranges (minimum & maximum values), and the frequencies were valid.

Outlier detection for the pre-and-post-tests was conducted using Mahalanobis Distance. As found, few records were potential multivariate outliers and were considered for elimination. However, after further analysis, including examining the stem-leaf graphs where limited Mahalanobis distances were actually significant, the UserID #s were not removed and all the responses from the 254 participants were kept for data analysis.

Demographic Analysis

For this study, data was collected on eight demographic indicators and a breakdown is shown in Table 13. Of the 254 participants, 192 (75.6%) were females while 62 (24.4%) were males, with most, 78 (30.7%) as well as 84 (33.1%) falling in the 65-69 and 70-74 age groups, respectively. Additionally, over 92% (206) reported using

computers for 15 or more years; 94% (239) have been using the Internet for at least 10 years; and over 79% (202) have been using Internet-enabled devices between five and 24 years. Moreover, 63% (160) have worked in a formal/corporate organization for at least 30 years, approximately 72% (183) have retired for less than 10 years, and majority have a Bachelor's or Master's degree, 31.5% (80) or 28.3% (72), respectively.

Table 13

Descriptive Statistics of the Population (N=254)

<i>Item</i>	<i>Frequency</i>	<i>Percentage</i>
<i>Gender</i>		
Males	62	24.4%
Females	192	75.6%
<i>Age Range</i>		
64 or under	35	13.8%
65-69	78	30.7%
70-74	84	33.1%
75-79	39	15.4%
80-84	12	4.7%
85-89	6	2.4%
90 or over	0	0%
<i>Years using Computers</i>		
5-9	4	1.6%
10-14	14	5.5%
15-19	40	15.7%
20-24	43	16.9%
25-29	53	20.9%
30-34	48	18.9%
35 or over	52	20.5%
<i>Years using the Internet</i>		
5-9	15	5.9%
10-14	33	13.0%
15-19	69	27.2%
20-24	72	28.3%
25-29	40	15.7%
30-34	15	5.9%
35 or over	10	3.9%
<i>Years using Internet-enabled Devices</i>		
1-4	23	9.1%
5-9	57	22.4%

10-14	74	29.1%
15-19	36	14.2%
20-24	35	13.8%
25-29	20	7.9%
30-34	9	3.5%
<i>Years Worked in Corporate/Formal Organization</i>		
1-4	16	6.3%
5-9	4	1.6%
10-14	14	5.5%
15-19	8	3.1%
20-24	23	9.1%
25-29	29	11.4%
30 or over	160	63.0%
<i>Years Since Retirement</i>		
0-4	115	45.3%
5-9	68	26.8%
10-14	29	11.4%
15-19	30	11.8%
20-24	5	2.0%
25-29	5	2.0%
30 or over	2	0.8%
<i>Highest Level of Education</i>		
High School	15	5.9%
Graduate/GED		
Some College	34	13.4%
Associate's Degree	14	5.5%
Bachelor's Degree	80	31.5%
Master's Degree	72	28.3%
Doctoral Degree	13	5.1%
Professional Degree	26	10.2%

Note. Due to rounding errors, some percentages may not add up to 100%

After the pre-analysis data screening process, the next step was to check for reliability and validity before moving on answer the research questions as well as to determine if the propositions were supported or not.

Reliability and Validity

Cronbach's Alpha and average variance extracted (AVE) in Smart PLS 3.0 were used as measures of internal reliability consistency and convergent validity, respectively

for the constructs used in this study. Cronbach's Alpha provides a measure or indication of how closely related or the inter-correlation of a set of items that are in the same group, while the AVE is the extent to which an item correlates positively with alternative items of the same construct (Hair et al., 2014). The results are shown in Table 14. Cronbach Alpha's values greater than 0.70 have been deemed acceptable reliability, and AVE values of at least 0.50 as acceptable validity (Hair et al., 2014; Levy & Danet, 2010). As shown in Table 14, all the constructs, except PRIT showed good reliability for the pre-test, while all, except PRIT and IM showed good reliability for the post-test. In both the pre-and-post-test, the PRIT showed moderate reliability (0.673 & 0.688, respectively), however, the post-test value was slightly higher than the pre-test value. There was a decrease in the IM value from 0.720 (acceptable) in the pre-test to 0.692 (moderately acceptable) in the post-test. Four out of the seven constructs showed acceptable values of at least 0.50 for the AVE in the pre-test, however, the remaining three showed values below 0.50. Those three constructs were PRIT, OACTA, and IM, with values of 0.181, 0.299, and 0.417, respectively. In the post-test, only three of the constructs, SCCA, CSE, and CyberSkills showed acceptable values of at least 0.50 for the AVE; all the others were below 0.50, and they all decreased in value from the pre-test values.

Table 14

Reliability (Cronbach's Alpha) and Validity (AVE) for this Study's Constructs (N=254)

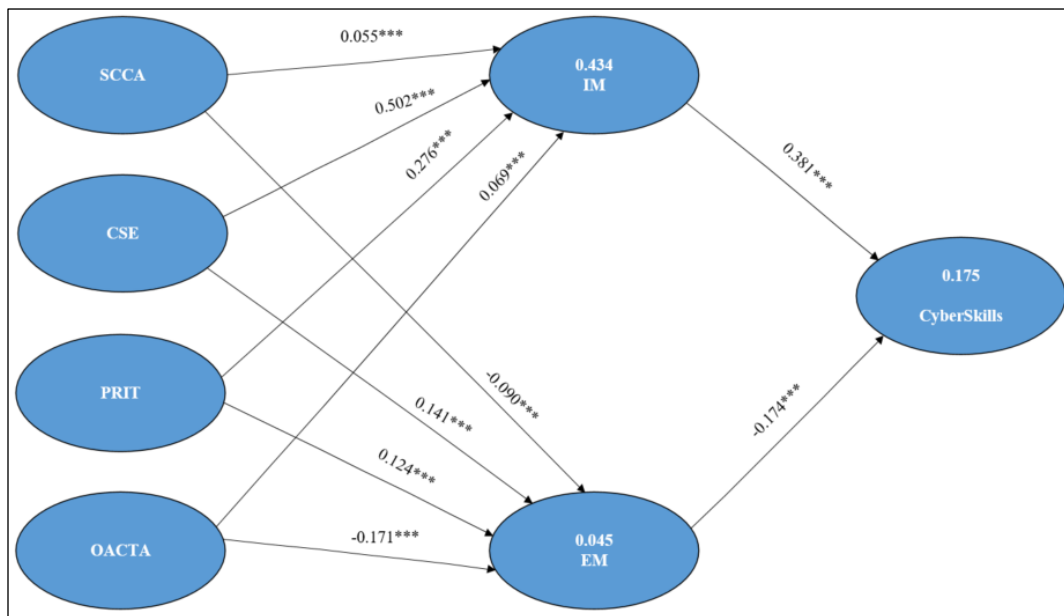
Construct	# of Items	Cronbach's Alpha		AVE	
		Pre-Test	Post-Test	Pre-Test	Post-Test
SCCA	8	0.895	0.929	0.514	0.619
CSE	3	0.747	0.815	0.502	0.595
PRIT	8	0.673	0.688	0.181	0.175
OACTA	17	0.887	0.873	0.299	0.277
IM	4	0.720	0.692	0.417	0.365
EM	4	0.802	0.835	0.506	0.277

CyberSkills	1	N/A	N/A	1.000	1.000
-------------	---	-----	-----	-------	-------

Research Questions and Propositions

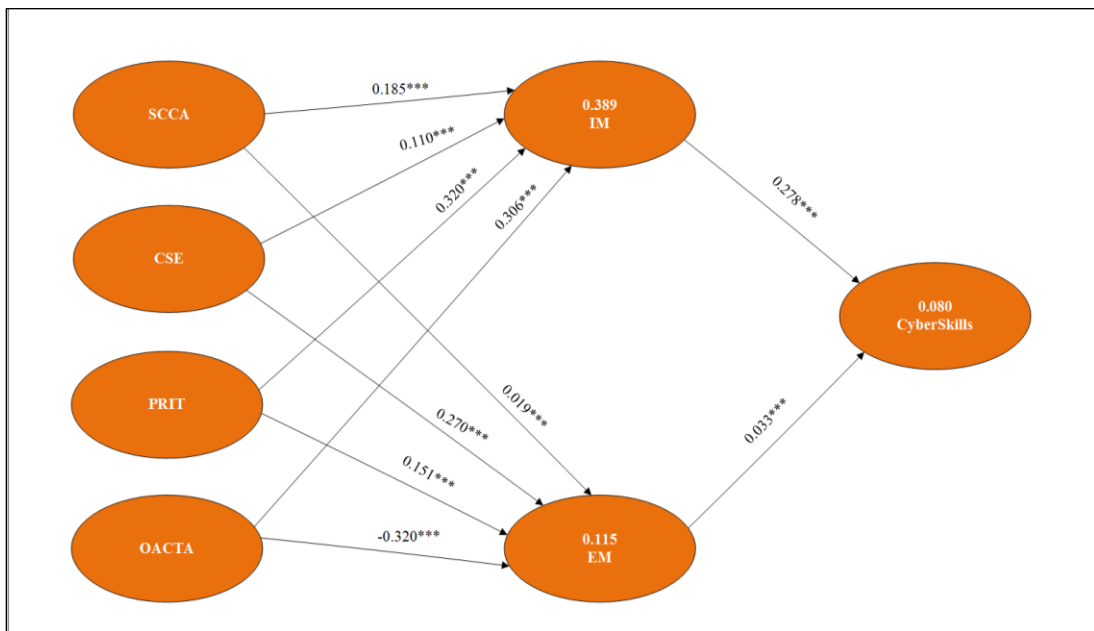
The main research question that this study addressed was: what is the contribution of senior citizens' SCCA, CSE, PRIT, and OACTA on their motivation (IM & EM) to acquire cybersecurity skills, as well as their cybersecurity skills level, while comparing it before and after cybersecurity awareness training? There were six specific research questions and seven propositions. As noted in Chapter 3, the relationships among the IVs and DVs, that is, the contributions of the IVs on the DV were assessed using path analysis in Smart PLS 3.0. Therefore, path analysis in SmartPLS 3.0 addressed RQ1 to RQ4, as well as P1 to P5. Figure 3 shows the results of the standardized path coefficients (β), along with the R-squared (R^2) values for the pre-test model, while Figure 4 shows the same types of results for the post-test model. In both models, the numbers that are noted above the arrows represent the path coefficients, while the R^2 values are noted within the given constructs where R^2 is applicable, that is, IM, EM, and Cybersecurity Skills Index. Path coefficients are used to estimate the strength of the relationship between constructs in a hypothesized causal model, while R^2 is a measure of the predictive accuracy of the model (Hair et al., 2014; Mertler & Vannatta, 2013). Path coefficients have standardized values between -1 and +1, with values that are closer to +1 depicting strong positive relationships, or values closer to -1 depicting strong negative relationships; values that are close to zero depict weak relationships (Hair et al., 2014). R^2 values of 0.75, 0.50, and 0.25 have been classified as substantial, moderate, and weak, respectively, and indicate the amount of variance in the DVs that can be explained by the IVs (Hair et al., 2014).

All paths on both the pre-test and post-test models were significant at $p < 0.001$, however, as shown in Figure 3 and Figure 4, for the pre-test and post-test, respectively, many of the paths had very low path coefficients. These low values indicate weak positive relationships for the paths with positive values, and weak negative relationships for the paths with negative values. Additionally, for the pre-test and post-test, IM has moderate R^2 values of 0.434 and 0.389 respectively, while EM has weak values of 0.045 and 0.115, respectively. Interestingly, while there was a decrease in the IM pre-test post-test R^2 values, there was an increase in the EM pre-test post-test R^2 values. In spite of this decrease/increase, the IM values remained in the moderate range while the EM values remained in the weak range (pre-post). Further, the pre-test model has an overall R^2 value of 0.175, while the post-test model overall R^2 value dropped to 0.080; in each case, these values indicate very weak predictive accuracy of each model.



*** $p < 0.001$

Figure 3. Outcome of the PLS Pre-Test Paths (N=254)



*** $p < 0.001$

Figure 4. Outcome of the PLS Post-Test Paths (N=254)

Proposition Testing

A summary of the results of the proposition testing is shown in Table 15, and each is discussed below. As noted before, all the paths on both the pre-test and post-test models were significant at $p < 0.001$, however, many of the paths had very low path coefficients.

P1_(a & b): There will be a significant positive contribution of senior citizens' SCCA on their (a) IM and (b) EM to acquire cybersecurity skills.

In both the pre-and-post-test, SCCA had a significant positive contribution on IM to acquire CyberSkills ($\beta=0.055$ & $\beta=0.185$, respectively, $p < 0.001$), hence, P1_(a) was fully supported. However, for the pre-test, SCCA had a significant negative contribution on EM to acquire CyberSkills, but a significant positive contribution on EM to acquire

CyberSkills for the post-test ($\beta=-0.090$ & $\beta=0.019$, respectively, $p < 0.001$). Hence, P1_(b) was partially supported in the pre-test, in that it was significant, but in the opposite direction, while it was fully supported in the post-test.

P2_(a & b): There will be a significant positive contribution of senior citizens' CSE on their (a) IM and (b) EM to acquire cybersecurity skills.

In both the pre-and-post-test, CSE had a significant positive contribution on both IM ($\beta=0.502$ & $\beta=0.110$, respectively, $p < 0.001$), and EM ($\beta=0.141$ & $\beta=0.270$, respectively, $p < 0.001$) to acquire CyberSkills, hence, there was full support for P2_(a & b). It is also noteworthy that while the proposition was supported in both the pre-and-post-test, the contribution of CSE on IM decreased in the post-test, while the contribution of CSE on EM increased in the post-test.

P3_(a & b): There will be a significant positive contribution of senior citizens' PRIT on their (a) IM and (b) EM to acquire cybersecurity skills.

In both the pre-and-post-test, PRIT had a significant positive contribution on both IM ($\beta=0.276$ & $\beta=0.320$, respectively, $p < 0.001$), and EM ($\beta=0.124$ & $\beta=0.151$, respectively, $p < 0.001$) to acquire CyberSkills, hence, there was full support for P3_(a & b).

P4_(a & b): There will be a significant positive contribution of senior citizens' OACTA on their (a) IM and (b) EM to acquire cybersecurity skills.

In both the pre-and-post-test, OACTA had a significant positive contribution on IM to acquire CyberSkills ($\beta=0.069$ & $\beta=0.306$, respectively, $p < 0.001$), hence, P4_(a) was fully supported. However, for both the pre-test and post-test, OACTA had a significant negative contribution on EM to acquire CyberSkills ($\beta=-0.171$ & $\beta=-0.320$, respectively,

$p < 0.001$). Hence, P4_(b) was partially supported in both the pre-and-post-test in that it was significant, but in the opposite direction.

P5_(a & b): There will be a significant positive contribution of senior citizens' (a) IM and (b) EM to acquire cybersecurity skills on their CyberSkills level.

There were also mixed results for this proposition. In both the pre-test and post-test, IM to acquire CyberSkills had a significant positive contribution on the CyberSkills ($\beta=0.381$ & $\beta=0.278$, respectively, $p < 0.001$), hence, P5_(a) was fully supported. However, for the pre-test, EM to acquire CyberSkills had a significant negative contribution on the CyberSkills, but a significant positive contribution on the CyberSkills for the post-test ($\beta=-0.174$ & $\beta=0.033$, respectively, $p < 0.001$). Hence, P5_(b) was partially supported in the pre-test, in that it was significant, but in the opposite direction, while it was supported in the post-test.

Table 15

Summary of Proposition Testing for P1 to P5 (N=254)

Prop. #	Path	Pre-Test			Post-Test		
		Path Coefficients	p-value	Supported	Path Coefficients	p-value	Supported
P1 _(a)	$\beta_{(SCCA \rightarrow IM)}$	0.055	0.000***	Yes	0.185	0.000***	Yes
P1 _(b)	$\beta_{(SCCA \rightarrow EM)}$	-0.090	0.000***	Partially	0.019	0.000***	Yes
P2 _(a)	$\beta_{(CSE \rightarrow IM)}$	0.502	0.000***	Yes	0.110	0.000***	Yes
P2 _(b)	$\beta_{(CSE \rightarrow EM)}$	0.141	0.000***	Yes	0.270	0.000***	Yes
P3 _(a)	$\beta_{(PRIT \rightarrow IM)}$	0.276	0.000***	Yes	0.320	0.000***	Yes
P3 _(b)	$\beta_{(PRIT \rightarrow EM)}$	0.124	0.000***	Yes	0.151	0.000***	Yes
P4 _(a)	$\beta_{(OACTA \rightarrow IM)}$	0.069	0.000***	Yes	0.306	0.000***	Yes
P4 _(b)	$\beta_{(OACTA \rightarrow EM)}$	-0.171	0.000***	Partially	-0.320	0.000***	Partially
P5 _(a)	$\beta_{(IM \rightarrow CyberSkills)}$	0.381	0.000***	Yes	0.278	0.000***	Yes
P5 _(b)	$\beta_{(EM \rightarrow CyberSkills)}$	-0.174	0.000***	Partially	0.033	0.000***	Yes

*** $p < 0.001$

P6_(a & b): There will be significant mean difference in the levels of senior citizens' CyberSkills level before (t_1) and after (t_3) the cybersecurity awareness training.

In order to examine the proposition that there will be significant mean difference in the levels of senior citizens' cybersecurity skill level before and after cybersecurity awareness training, a one-way between-groups ANOVA was conducted. The results indicate that the proposition was supported as a significant mean difference was observed in the levels of senior citizens' cybersecurity skill level before and after cybersecurity awareness training, $F(df = 506) = 42.14, p < .001$. Further, as shown in Figure 5, the mean cybersecurity skill score before the training was lower ($M = 59.67, SD = 8.56$) than the after training cybersecurity skill score mean ($M = 64.51, SD = 8.24$).

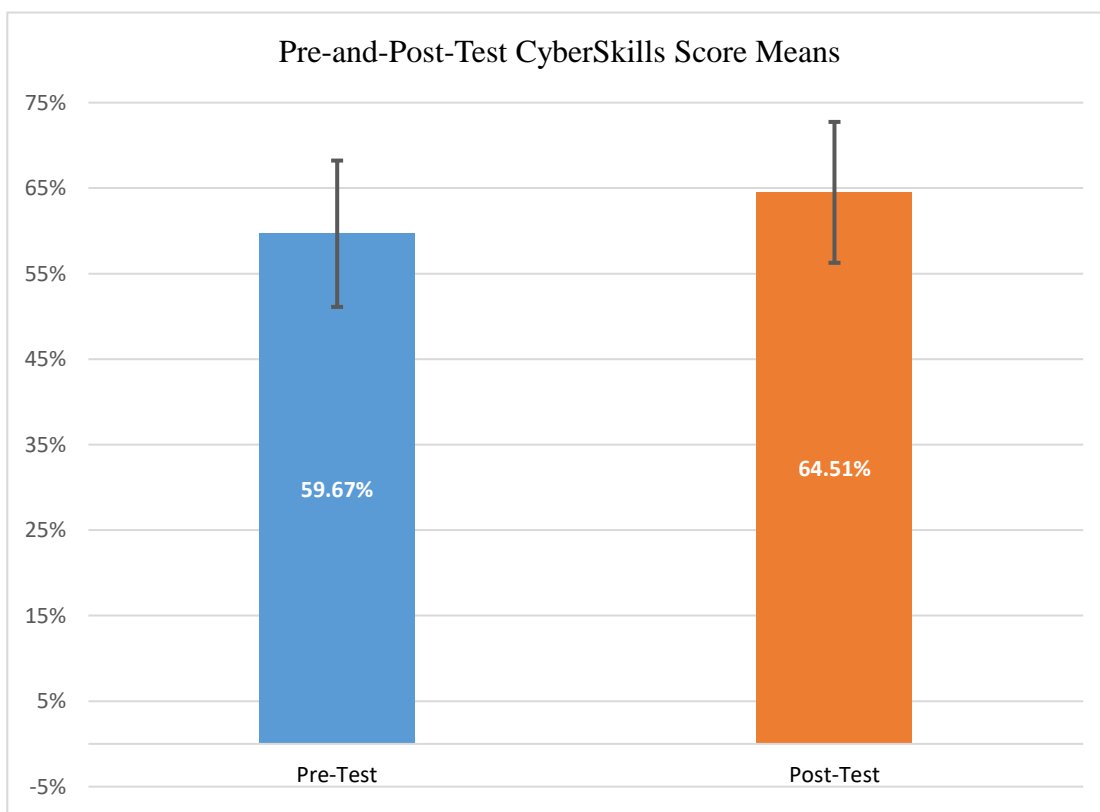


Figure 5. Pre-and-Post-Test CyberSkills Score Means (N=254)

P7_(a to h): There will be significant mean difference in the levels of senior citizens' cybersecurity skill level before (t_1) and after (t_3) the

cybersecurity awareness training, when controlled for the following eight demographic indicators: (a) age, (b) gender, (c) years of using computers, (d) years of using the Internet, (e) years of using Internet-enabled mobile devices, (f) years of working in corporate or formal organization, (g) years since retiring, and (h) level of education.

A one-way ANCOVA was conducted to determine a statistically significant difference in the levels of senior citizens' CyberSkills level before and after cybersecurity awareness training, when controlled for the eight aforementioned demographic indicators. Except for years using computers which was significant, $F(df = 1) = 11.052$, $p = .001$, all the other demographic indicators were not significant, as depicted in Table 16. Therefore, $P7_{(a, b, d, e, f, g, \& h)}$ were supported, while $P7_{(c)}$ was not supported.

Table 16

ANCOVA: Tests of Between-Subjects Effects - Dependent Variable: CyberSkills (N=254)

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Age	110.60	1	110.60	1.691	0.194
Gender	55.63	1	55.63	0.851	0.357
Years of Using Computers	722.86	1	722.86	11.052	0.001**
Years of Using the Internet	148.21	1	148.21	2.266	0.133
Years of Using Internet-enabled Devices	104.53	1	104.53	1.598	0.207
Years Working in a Formal/Corporate Organization	131.39	1	131.39	2.009	0.157
Years Since Retiring	120.00	1	120.00	1.835	0.176
Highest Level of Education	208.06	1	208.06	3.181	0.075
PrePost	2899.25	1	2899.25	44.327	0.000***

** $p < 0.005$, *** $p < 0.001$

Summary

This chapter presented the results of this study. First, the results of Phase 1 in which the validation procedures for the survey instrument were outlined. This included the outcomes from the expert panel review, in which some adjustments were made to the survey instrument. Next the results of Phase 2 in which the pilot test was conducted was outlined. The pilot test did not necessitate any changes/modifications to the survey instrument, however, based on feedback, some modifications were made to the main data collection procedures. These changes included removing the mandatory attendance to the computer lab to do both the pre-and-post-tests. As a result, participants, were given the option to complete the pre-test outside of the lab or attend the lab, plus all participants were required to complete the post-test outside of the lab. Given the fact that the participants were senior citizens, this encouraged participation as it limited the number of times that they had to physically attend the lab; in the end, they were only required to attend the lab for the face-to-face 2-hours cybersecurity awareness training. Finally, Phase 3, which included the main data collection of the pre-and-post training measures that addressed the research questions, including pre-analysis data screening and data analysis was presented.

Of the seven propositions that were presented, five were tested in Smart PLS 3.0, while ANOVA and ANCOVA in SPSS were used to test the remaining two. Of the five that were tested in Smart PLS 3.0, the results show that two were fully supported in both the pre-and-post-tests. These included P2_(a & b) and P3_(a & b). While the remaining propositions were not fully supported, none was rejected, as they were either fully supported in the pre-test and partially supported in the post-test, or vice-versa. P6_(a & b)

was supported in ANOVA and $P7_{(a \text{ to } h)}$ was mostly supported in ANCOVA; the only demographic indicator that was found to be significant was years using computers. Some very interesting and unexpected results were found, and will be further discussed in the next chapter.

Chapter 5

Conclusion, Implications, Recommendations, and Summary

Conclusions

Senior citizens make up one of the fastest growing groups of Internet users, yet research has shown that many seniors venture into cyberspace without the requisite skills on how to protect themselves against cyber-attacks, thus, making them very vulnerable to those types of attacks (Grimes et al., 2010; Iyer & Eastman, 2006; Perrin & Duggan, 2015; Wagner et al., 2010). With this knowledge of senior citizens' lack of cybersecurity skills, cyber-criminals often target and exploit them online, with one in five American senior citizens being a victim of financial fraud, costing more than \$2.6 billion per year (Grimes et al., 2010; Willis, 2015). In response, this study addressed the problem of the increase in the success of cyber-attack vectors due to limited cybersecurity awareness and skills among Internet users, especially senior citizens, which ultimately causes them significant financial losses (Abbasi et al., 2010; D'Arcy et al., 2009; Purkait et al., 2014). This study built on the work of previous researchers who recommended further research into promoting cybersecurity awareness among HCU's so that they could develop the necessary skills to protect themselves from the growing threats to their home computers (Furnell et al., 2007). Cybersecurity awareness is essential in training and developing the cybersecurity skills of Internet users, which when acquired, would reduce the cybersecurity vulnerabilities that users face when they use the Internet (Carlton & Levy,

2015; D'Arcy et al., 2009; Furnell et al., 2007; Shillair et al., 2015). Carlton and Levy (2015) identified nine cybersecurity skills that were needed by non-IT professionals to counter cyber-attacks, and subsequently developed as well as validated a hands-on scenarios-based application that would measure those cybersecurity skills. Therefore, the main goal of this research study was to empirically assess the contributions of senior citizens' SCCA, CSE, PRIT, and OACTA on their motivation (IM & EM) to acquire cybersecurity skills, as well as their Cybersecurity Skills level, while comparing each before and after cybersecurity awareness training. From this main goal, six specific goals were developed, with each having a matching research question and proposition. The goals, research questions and propositions were addressed using a three-phased approach. The survey instrument was developed and validated in phase one; pilot testing was done in phase two, and the main data collection, along with the data analysis, and interpretation was done in phase three. As part of phase three, the MyCyberSkills™ iPad app that was developed and validated in the Carlton and Levy (2015) study was used to assess the cybersecurity skills of the senior citizens.

Discussion

In addressing the goals and answering the research questions of this study, Smart PLS 3.0 was used to assess the paths in the research model for both the pre-and-post-test, plus ANOVA and ANCOVA in SPSS were used to evaluate group differences. The results revealed some very interesting, and in some cases, unexpected findings. For example, it was interesting, and unexpected to find that while all paths on both models were significant at $p < 0.001$, many of the paths had very low path coefficients, indicating

weak relationships, and low R^2 values, indicating weak predictability of the model. Another interesting observation was that although the path coefficients and R^2 values were lower than expected, most of them were in the direction as proposed. A possible explanation for these findings can be attributed to the unit of analysis, that is, senior citizens. Previous research had alluded to differences in senior citizens regarding factors that might motivate them to acquire new skills and how the skills can be acquired (Phipps et al., 2013). Ng (2007) also reported that within the context of training senior citizens, there were some challenges, which include motivating them to develop new computing skills, and once the skills were developed, for them to keep on practicing them. Further, due to challenges that are unique to senior citizens because of their age, they required special consideration when it came to training (Greengard, 2009; Lam & Lee, 2006). Some of the challenges were cognitive as well as physical, such as fading memory, slower speed at processing information, poor vision, and slow motor skills that resulted from chronic conditions, e.g. weak muscles (Goodwin, 2013; Greengard, 2009; Lam & Lee, 2006). This study may not have taken into account all the special considerations, and as such, some of the findings were different from what would have been expected if a similar study was done with a younger population or with persons who were mostly still in the workplace. The following sub-sections present a detailed discussion of each result.

Proposition 1_(a & b)

P1_(a) was fully supported in both the pre-and-post-tests, however, P1_(b) was partially supported in the pre-test, but fully supported in the post-test. As proposed, in both the pre-and-post-test, SCCA had a significant positive contribution on IM to acquire CyberSkills ($\beta=0.055$ & $\beta=0.185$, respectively, $p < 0.001$). On the other hand, and

unexpectedly, for the pre-test, SCCA had a significant negative contribution on EM to acquire CyberSkills, but a significant positive contribution on EM to acquire CyberSkills for the post-test ($\beta=-0.090$ & $\beta=0.019$, respectively, $p < 0.001$). A possible explanation to this unexpected finding in the pre-test could be that the awareness that senior citizens had of cyber-attacks that they perceived to be too dangerous would cause them to be extrinsically demotivated to even want to acquire the skills to counter those attacks. However, through the training they realized that it was even more dangerous to ignore those cyber-attacks, therefore, they became motivated to acquire the cybersecurity skills simply because they are required. Reports in literature indicated that there was a relationship between cybersecurity awareness and motivation (Claar & Johnson, 2012; McCrohan et al., 2010). While some research indicates a positive relationship in that increased cybersecurity awareness will influence a user's ability to detect cyber-attacks and motivate mitigating actions (Claar & Johnson, 2012; D'Arcy et al., 2009; McCrohan et al., 2010), others have reported a negative relationship. For example, White (2015) reported that an increase in a user's cybersecurity awareness also increased the number of reported cybersecurity incidents, while Wolf et al. (2011) found that the effectiveness of cybersecurity awareness diminished over time. In spite of the weak relationships indicated by the low path coefficients, the findings from this study support the positive relationship reports, as overall, there was a stronger positive contribution of SCCA to both IM and EM to acquire CyberSkills, after the cybersecurity awareness training.

Proposition 2_(a & b)

P2_(a & b) were fully supported in both the pre-and-post-tests. As proposed, in both the pre-and-post-test, CSE had a significant positive contribution on both IM ($\beta=0.502$ &

$\beta=0.110$, respectively, $p < 0.001$), and EM ($\beta=0.141$ & $\beta=0.270$, respectively, $p < 0.001$) to acquire CyberSkills. In spite of the weak relationships indicated by the low path coefficients, the support for this proposition in this study is consistent with findings from prior research that indicate a positive relationship between CSE and motivation (Hasan & Ali, 2004; Rhee et al., 2009; Zhang & Espinoza, 1998). However, it was surprising and unexpected to find that the contribution of CSE on IM to acquire CyberSkills decreased in the post-test. It should also be noted that the contribution of CSE on EM to acquire CyberSkills increased in the post-test. One possible explanation for this finding, i.e. the drop in contribution of CSE on IM to acquire CyberSkills in the post-test could be that, given the demographics of the participants, i.e. senior citizens, the knowledge gained from the cybersecurity awareness training revealed their lack of the requisite skills, which in turn impacted their confidence levels to master the skills. Therefore, after the training, they were more extrinsically motivated, i.e. to get a better score on the post-test, than they would be intrinsically motivated to acquire cybersecurity skills, for the sheer fun of it. When users find that they lack confidence in their skills, they are more reluctant to participate in activities and would abandon the activities when faced with difficulties (Bandura, 1986). This implies that, within the context of this study, the participants would be more likely to abandon difficult cybersecurity tasks simply because they enjoy it (intrinsic), but would possibly persist for external reasons (extrinsic), e.g. to get a better score. During the training sessions, some of the seniors indicated that although some of the scenario tasks were a little difficult to relate to, they would try their best to get a better score on the post-test. Also, due to the problems that some of them had with the time-out and server connection issues, their confidence levels in their abilities to do the

tasks may have diminished but they persisted because they wanted to improve their scores. Further, as a result of some sharing their pre-test scores, others may have aimed to out-do their peers on the post-test. All these factors seem to support the increase in extrinsic motivation after the training.

Proposition 3_(a & b)

P3_(a & b) were fully supported in both the pre-and-post-tests. As proposed, in both the pre-and-post-test, PRIT had a significant positive contribution on both IM ($\beta=0.276$ & $\beta=0.320$, respectively, $p < 0.001$), and EM ($\beta=0.124$ & $\beta=0.151$, respectively, $p < 0.001$) to acquire CyberSkills. The literature reports contradictory findings regarding the relationship between perceived risk and motivation. For example, Liang and Xue (2010) found a negative interaction between the levels of a user's perceived risk and the user's motivation to take mitigating actions, while Johnston and Warkentin (2010) suggested that when users were made aware of risks regarding cybersecurity threats, e.g. in this study, identity theft, the users would be more motivated to take mitigating actions. Although the findings in this study show a smaller increase in the PRIT to EM contribution than to the IM contribution after the training, both paths in both models show an overall increase in contribution. According to Greengard (2009) and Jones (2001), identity theft is one of the common risk perceptions of senior citizens when they use the Internet, and coupled with their limited cybersecurity skills, they feel overwhelmed, frustrated as well as demotivated when they use the Internet. As a result of the training, the senior citizens demonstrated an increase in both intrinsic and extrinsic motivation to acquire cybersecurity skills as they can both enjoy protecting themselves from identity theft-related attacks as well as protecting themselves because it is now a

requirement. This finding, therefore, is consistent with findings from prior research that indicate that there is a positive relationship with PRIT and motivation (Herath & Rao, 2009; Johnston & Warkentin, 2010).

Proposition 4_(a & b)

P4_(a) was fully supported in both the pre-and-post-tests, however, P4_(b) was partially supported in both the pre-and-post-tests. As proposed, in both the pre-and-post-test, OACTA had a significant positive contribution on IM to acquire CyberSkills ($\beta=0.069$ & $\beta=0.306$, respectively, $p < 0.001$). However, unexpectedly, for both the pre-test and post-test, OACTA had a significant negative contribution on EM to acquire CyberSkills ($\beta=-0.171$ & $\beta=-0.320$, respectively, $p < 0.001$). This finding indicates that as the computer technology attitudes of senior citizens increase, they would become more intrinsically motivated to acquire cybersecurity skills, alternatively, as their attitudes increase, they would become less extrinsically motivated to acquire cybersecurity skills, even after cybersecurity awareness training. Although this finding is unexpected, there are also reports in literature of contradictory findings regarding the technology attitudes of senior citizens and the outcomes of computer training (Broady et al., 2010). Iyer and Eastman (2006) reported that due to the negative attitudes of senior citizens towards technology, they were less likely to use the Internet, and as such probably would not try to access it on their own. Within the context of this study, this implies that as a result of the negative attitudes of senior citizens, they would be less intrinsically motivated to acquire skills on how to effectively use the Internet, i.e. use it because they enjoy the experience, than for them to use it because they are required or forced to use it, i.e. extrinsic. On the other hand, Chen and Chan (2013) as well as Schmidt et al. (2014)

indicated that senior citizens had an overall positive attitude towards technology, and were motivated to use it for both intrinsic and extrinsic reasons, especially in light of the many benefits they get from using it. Some of the benefits are intrinsic, e.g. satisfying their general curiosity and interest about new technology, as well as playing games for enjoyment, while others are extrinsic, e.g. allowing them to lead healthier lives, being more socially engaging by allowing them to connect remotely with family and friends as well as being more independent, e.g. allowing them to access services such as medical, financial, shopping, entertainment, and sports (Chen & Chan, 2013; Gonzalez et al., 2015; Wagner et al., 2010). There are more reports in the literature that support a positive relationship between attitudes and extrinsic motivation in senior citizens than intrinsic motivation. However, the findings of this study are not consistent with such reports, and, hence, require further investigation.

Proposition 5_(a & b)

P5_(a) was fully supported in both the pre-and-post-tests, however, P5_(b) was partially supported in the pre-test, but supported in the post-test. As proposed, in both the pre-test and post-test, IM to acquire CyberSkills had a significant positive contribution on the CyberSkills ($\beta=0.381$ & $\beta=0.278$, respectively, $p < 0.001$). Unexpectedly, for the pre-test, EM to acquire CyberSkills had a significant negative contribution on the CyberSkills, but, as expected, a significant positive contribution on the CyberSkills for the post-test ($\beta=-0.174$ & $\beta=0.033$, respectively, $p < 0.001$). These results were interesting in that they were both mixed and unexpected. This implies that prior to the cybersecurity awareness training, any increase in external motivational factors would cause a decrease in their CyberSkills, however, after the training, any increase in the

external motivational factors would result in an increase in their CyberSkills. This could be due to the fact that, through the training, the seniors were now more aware of the dangers of ignoring those external motivational factors, especially in light of the fact that using the Internet has now become a part of everyday life, i.e. required. After the training, some of the seniors had expressed alarm at the knowledge of the capabilities of cyber-criminals and the ease with which cyber-attacks can occur, irrespective of the amount of time or the type of activities that they do online. Some stated that they thought that only in cases where they spend an enormous amount of time as well as performed activities of a sensitive nature, e.g. banking, would cause them to be likely cyber-attack preys. Activities such as simply checking emails or using social media applications on especially free/public WiFis were not considered risky until after the training. This knowledge would cause the senior citizens to be more extrinsically motivated because they would not want, for example, to become victims of cyber-crimes. It should also be noted that while the relationship between IM and CyberSkills remained positive for the post-test, there was a decrease in the strength of the relationship, again implying that after the training, EM (resulting from external factors, e.g. fear of identity theft) was stronger than IM (resulting from internal factors, e.g. enjoyment). There is some support in the literature for the negative contribution of EM to CyberSkills that was observed in the pre-test. Perception of identity theft was one of the common fears of senior citizens when they use the Internet, and this fear, coupled with their limited cybersecurity awareness and skills, cause them to feel overwhelmed, frustrated as well as demotivated when they use the Internet (Greengard, 2009; Iyer & Eastman, 2006; Jones, 2001). However, after the cybersecurity awareness training, there was a positive contribution of EM to

CyberSkills, which is also consistent with prior research. For example, Goodwin (2013) indicated that although senior citizens displayed interest in computers and the Internet, they were demotivated to use them because they did not have the requisite skills to complete the required tasks. This implies that, with the requisite cybersecurity skills (as occurred after the training), senior citizens would be motivated to use the Internet. The cybersecurity awareness training provided the senior citizens with some of the requisite cybersecurity skills, hence, their motivation level increased as they were better able to protect themselves from cyber-attacks. Further, prior researchers indicated that it was important to identify the factors that would motivate senior citizens to acquire cybersecurity skills (Goodwin, 2013; Grimes et al., 2010; Marquié et al., 2002). The findings from this study indicate that, after cybersecurity awareness training, extrinsic motivational factors provided a stronger percentage change (118.97%) on motivation to acquire CyberSkills than intrinsic motivational factors (-27.03%).

Assessment of R² Values

As shown in Figure 3 and Figure 4, for both the pre-test and post-test, IM had moderate R² values of 0.434 and 0.389 respectively, while EM had weak values of 0.045 and 0.115, respectively. Interestingly too, while there was a decrease in the IM pre-test post-test R² values, there was an increase in the EM pre-test post-test R² values. In spite of this decrease/increase, the IM R² values remained in the moderate range while EM R² values remained in the weak range. This means that 43.4% of the variability in IM to acquire cybersecurity skills can be explained by the variability in the IVs (SCCA, CSE, PRIT, & OACTA) for the pre-test, while in the post-test, it fell to 38.9%, with CSE as the only IV to show a decrease in contribution strength. Similarly, 4.5% of the variability in

EM to acquire cybersecurity skills can be explained by the variability in the IVs (SCCA, CSE, PRIT, & OACTA) for the pre-test, while it increased to 11.5% in the post-test; OACTA was the only IV that decreased. Although the values are low, they suggest that after the cybersecurity awareness training, the seniors were more extrinsically motivated to acquire cybersecurity skills than they were intrinsically motivated. This could mean that their increased knowledge of the dangers of cyber-attacks through the training had a greater impact on their EM to acquire cybersecurity skills, i.e. acquiring cybersecurity skills because it is a requirement, than on their IM to acquire cybersecurity skills, i.e. acquiring cybersecurity skills for fun or enjoyment. This finding with senior citizens, who are increased in age, is also consistent with prior research where it was found that intrinsic motivation decreased as age increased (Lepper et al., 2005; Ryan & Deci, 2000). One may question if this decrease/increase would be sustained over a period of time, or, if it was due to the fact that the recent knowledge of the dangers of cyber-attacks manifested itself in a “temporary” decrease in intrinsic motivation and an increase in extrinsic motivation. It is possible that this question can be answered in future research in which a longitudinal study is conducted.

The overall pre-test model had an R^2 value of 0.175, while the overall post-test model had an overall R^2 value of 0.080, which in each case, indicated a very weak to negligible predictive accuracy of each model. Since the R^2 values indicate the amount of variance in the DV that can be explained by the IVs, it can be concluded that both IM and EM are weak indicators at predicting the cybersecurity skills of senior citizens. Therefore, other factors than IM and EM have stronger impacts on the cybersecurity skills of seniors, and should be further investigated. Prior research has also shown that

there was a positive relationship between Internet users' motivation to take active roles towards mitigating cyber-attacks and their cybersecurity skills level (Holt & Turner, 2012; Inan et al., 2016, Mohamed & Ahmad, 2012). Further, Mohamed and Ahmad (2012) stated that when Internet users were confident that they possessed cybersecurity skills, they would be motivated to play active roles to protect themselves and their PII in the event of cybersecurity threats. Additionally, Phipps et al. (2013) concluded that intrinsic motivators may be insufficient to increase the motivation to acquire new skills in senior citizens. Hence, since acquiring skills such as cybersecurity skills was new for senior citizens, other factors, specifically extrinsic motivators that would motivate senior citizens to acquire new skills should be investigated (Phipps et al., 2013). While the findings in this study support the aforementioned claims, i.e. a positive relationship exists, the strength of the relationships of the IVs was unexpected, and, as mentioned before, this can possibly be explained by the demographics of the participants, in that they were senior citizens, with a mean age of 70.54 years, and approximately 28% had been retired for at least 10 years. It was expected that the R^2 values would have been higher as well as the strengths of the contributions would have been stronger. However, taking into account the special considerations that should be given to senior citizens that were mentioned in prior research, for example the challenges that they face due to their age, the results are within reasonable expectations (Goodwin, 2013; Greengard, 2009; Lam & Lee, 2006). The feedback after the training was positive and all the participants indicated that they acquired a lot of knowledge. However, some also stated that it was a lot of information to absorb and process in two hours and that the training should be split in multiple sessions, and include some more hands-on activities. Therefore, although they

learned a lot during the sessions, they experienced difficulties recalling what they had learned when they were doing the post-test. Additionally, some mentioned having difficulties with server connection problems and the screens freezing multiple times during the assessment. This may have caused them to become frustrated in trying to finish all the tasks and that could have contributed to decreased intrinsic motivation as frustration during computer use has been associated with decreased motivation and decreased higher-level cognitive functions (Goodwin, 2013).

Proposition 6_(a & b)

In order to examine the proposition that there will be significant mean difference in the levels of senior citizens' CyberSkills level before and after cybersecurity awareness training, a one-way between-groups ANOVA in SPSS[®] was conducted. This was done to determine if the cybersecurity awareness training had an impact on mitigating the cybersecurity risks. The findings showed that the ANOVA was significant, $F(df = 506) = 42.14, p < .001$, and indicated that the cybersecurity awareness training was effective in increasing the CyberSkills level of senior citizens. Hence, the proposition was supported. This was also evident in the significant improvement in their mean scores from 59.67% prior to the training to 64.51% after the training. This finding is consistent with findings in prior research where increasing the cybersecurity awareness of Internet users was found to empower them with the ability to detect and avoid cyber-attacks, as well as increase their abilities to detect cyber-attacks, and hence, take mitigating actions (Albrechtsen & Hovden, 2010; Choo, 2011; D'Arcy et al., 2009; Kritzinger & von Solms, 2010; Rahim et al., 2015). Similarly, this finding supports the recommendation from prior researchers that Internet users should increase their cybersecurity awareness in order to

acquire the skills to counter the dangers of cyber-attacks (Jones & Heinrichs, 2012; White, 2015). The increase in mean CyberSkills scores after the training is also evidence that other factors than IM and EM have stronger impacts on the cybersecurity skills of seniors, given the low R^2 values of both the pre-test-and-post-test models. These other factors should be further investigated.

Proposition 7_(a to h)

A one-way ANCOVA was conducted to determine a statistically significant difference in the levels of senior citizens' CyberSkills level before and after cybersecurity awareness training, when controlled for the following eight demographic indicators: age, gender, years of using computers, years of using the Internet, years of using Internet-enabled mobile devices, years of working in corporate or formal organization, years since retiring, and level of education. This was done to determine if there were any indirect effects of the IVs on the DV, through the demographic indicators. Except for years using computers which was significant, $F(df = 1) = 11.052$, $p = .001$, all the other demographic indicators were not significant, as depicted in Table 16. Therefore, $P7_{(a, b, d, e, f, g, \& h)}$ were supported, while $P7_{(c)}$ was not supported. This finding indicates that there were little or no indirect effects of the IVs on the DV, through the demographic indicators, and indicates that the relationships between the IVs and DV would be the same when there is control for the demographic indicators. There have been contradictory results reported in literature regarding the interactions of demographic indicators such as the ones used in this study and cybersecurity issues. For example, Carlton (2016) reported that the level of education and years using computers were significant demographic variables as it related to cybersecurity skills level of non-IT professionals.

Additionally, gender and level of education were reported as not having significant impacts on the ability of Internet users to correctly identify a phishing website, while age had an inverse relationship with the Internet user's ability to correctly identify a phishing Website (Purkait et al., 2014).

Limitations of the Study

Similar to other studies, this study has several limitations. One key limitation is generalization of the findings in that the study did not consider other factors such as culture, language, socio-economic conditions, and access to technology. Additionally, since there was approximately only one quarter (25%) of the sample who were males, the findings may not be representative of male senior citizens in the general population. The online tool that was used to assess the cybersecurity skills of the senior citizens, namely MyCyberSkills, had some shortcomings. The feedback from most of the participants was that the scenarios that were used to test the skills were more suited for persons who were still in the workforce, and since over 50% of them had retired for more than five years, many of them found it difficult to relate to the scenarios. Additionally, some scenarios were split over more than one window, and some participants did not retain what was indicated in the previous window, plus there were no options to go back. In such cases, participants randomly clicked on answers. In other cases, the images and screen shots that were included in some scenarios were difficult to read, therefore, in such cases, again, the participants randomly chose answers to the best of their abilities, especially those with vision issues. Another limitation was the length of time that it took to complete both the survey instrument and the MyCyberSkills app. Some participants became tired towards

the end of the app and did not pay much attention to the answers that they selected. In the initial stages of the data collection, there were server time-out and connection issues causing the screens to freeze frequently – this frustrated some of the participant and it lengthened the time to complete the assessment.

Future Research

Based on the findings in this study, future research can continue to explore the factors that will motivate senior citizens to acquire cybersecurity skills so that they can adequately protect themselves from cyber-attacks. While a number of studies have focused on the effects on senior citizens of acquiring skills to use computing technologies such as the Internet, very few have focused on acquiring cybersecurity skills, which would empower them to identify as well as mitigate the evolving problem of cyber-attacks (Grimes et al., 2010; Hart et al., 2008; Lam & Lee, 2006; Ng, 2007). Future research can also consider developing a shorter cybersecurity assessment tool with scenarios that are more relevant to retirees and/or persons who are outside of the organizational context. The feedback from many of the participants was that they did not feel that their cybersecurity skills score, especially after the training, reflected what they had learned as it was still difficult to relate to the given scenarios. After the development of such assessment tool, this study can be repeated to see if similar results will be seen. For this study, it was very difficult to find a survey instrument with items that measured cybersecurity awareness within the context of HCUs, that is, for persons who accessed the Internet from a personal computer for personal use outside the work environment, and is self-responsible to secure the computer in terms of malware protection, updates,

patches etc. (Kritzinger & von Solms, 2010). Most instruments that were found were used within the organizational context. Therefore, future research could develop and validate a cybersecurity awareness instrument for use within the HCU context, especially since cybersecurity awareness is now applicable to all Internet users.

Implications and Recommendations

This study has several implications from both a theoretical and practical standpoint.

Theoretical Implications

Theoretically, using SDT as the theoretical lens within the InfoSec domain, this study adds to the body of knowledge in attempting to understand human motivation to acquire new skills. Specifically, it will add to the body of knowledge on the factors that can motivate senior citizens to acquire cybersecurity skills so that they will be empowered to mitigate the effects of cyber-attacks when the attacks occur. Additionally, the findings from this study can also highlight and shed some light on the different responses that exist among younger populations, persons in organizations (employees) and senior citizens as it relates to cybersecurity issues. Most prior studies have largely focused on employees and younger populations in the areas of cybersecurity. Therefore, this study contributes to an improved understanding that the approaches and strategies towards addressing cybersecurity issues should be different for senior citizens, especially since there are reports of significant increases in Internet use among seniors. Further, there is also an increase in the number of persons in the older population who are pursuing learning opportunities that arise from the information age and from changes in

technology (Phipps et al., 2013). The results of this study can also be valuable in assisting other researchers who attempt to investigate cybersecurity awareness and skills within the context of older adults or senior citizens. This is so as the data was collected from a wide cross-section of participants whose demographics is representative of such populations.

Practical Implications

Prior research had found that although there were many research projects that identified limited awareness of cybersecurity countermeasures as a problem among HCUs, there was little amount of research done on designing and implementing appropriate cybersecurity awareness programs to solve this problem (Kritzinger & von Solms, 2010). Further, Grimes et al. (2010) called for further research into determining what types of cybersecurity awareness training would be most effective in training senior citizens who had limited cybersecurity awareness and skills. One of the significant practical implications of this study is that the training content can be developed into a blue-print training model that can be administered to HCUs, including senior citizens, across the globe. The content for the training used in this study was based on the essential cybersecurity skills needed by non-IT professionals that were identified and validated in the Carlton and Levy (2015) study. This also means that the training content can be easily modified and administered to personnel who are still in the workforce. Relevant updates can be made to the content as new cybersecurity threats arise. Another practical implication is that both the training content and the MyCyberSkills™ iPad app can be used together to address as well as assess cybersecurity issues among Internet users, regardless of context or age group. Care should be taken that, especially when training senior citizens, the training sessions should be conducted in small groups, the content

broken up into small chunks to be delivered over a period of time so that too much information is not given in the same session, and time be given for social interactions among the trainees. Ng (2007) cautioned against one-shot intervention programs when trying to promote the use of computing technologies and acquiring of new skills in older adults. The Ng (2007) study also emphasized the importance of the inclusion of social embeddedness in programs that were designed to develop motivation to use computing technologies and acquire new skills among older adults. The training sessions should also include hands-on activities, for example, having the senior citizens configuring their own devices to meet basic cybersecurity requirements. This could increase their motivation to acquire the new cybersecurity skills and should also promote continuance of use of the acquired skills. There can also be a “Train the Trainer” model where seniors who are more adept with technology can be trained and they in turn would provide the training to the other seniors. This should increase the reception from the trainees and the effectiveness of the training as the seniors would be receiving the training from their peers who should have a better understanding of the issues that seniors face in training programs (Chen & Chan, 2013). The aforementioned recommendations, along with the training content can be useful to law enforcement and other agencies that work with senior citizens in their efforts to address as well as attempt to reduce the number of reported cases relating to cybersecurity issues amongst senior citizens. Corporate organizations also need to take note as the population ages and more corporate services are being migrated to the Internet. For example, senior citizens with limited awareness of cybersecurity countermeasures often use devices that are not well protected to access corporate services, e.g. banking information. The use of these less protected devices

coupled with the limited awareness of the senior citizens can be easily manipulated by cyber-criminals in launching cyber-attacks on corporate computer systems (White, 2015). The corporate organizations can also partner with public agencies that work with senior citizens in assisting to provide the resources to increase cybersecurity awareness and skills amongst senior citizens. Senior citizens will also benefit in that, as a result of the cybersecurity awareness training, they would be better able to identify and mitigate the effects of cyber-attacks, which has had devastating effects on their lives. Hence, this increased awareness should cause a reduction in the success of cyber-attacks vectors that result from limited awareness of cybersecurity countermeasures among senior citizens.

Summary

Billions of dollars in losses have been accrued to Internet users as a result of cyber-attacks that exploit human vulnerabilities, for example, phishing and identity theft attacks (Abawajy, 2014; Hong, 2012). Senior citizens have been identified as one of the most vulnerable groups of Internet users who are prone to cyber-attacks, and this results from the fact that they have limited cybersecurity awareness and skills (Claar & Johnson, 2012; Grimes et al, 2010). Therefore, this study addressed the research problem of the increase in the success of cyber-attack vectors due to limited cybersecurity awareness and skills among Internet users, especially senior citizens, which ultimately causes them significant financial losses (Abbasi et al., 2010; D'Arcy et al., 2009; Purkait et al., 2014). Cybersecurity awareness is essential for senior citizens as a countermeasure strategy to combat and mitigate the cyber-attacks that they face (Choo, 2011). This study empirically assessed the factors that contributed to senior citizens' motivation to acquire

cybersecurity skills, as well as assessed their actual cybersecurity skills levels using a previously developed and validated scenario-based iPad application (Carlton & Levy, 2015; Carlton et al., 2016). The findings from this study provided a better understanding of the factors that will motivate senior citizens to acquire cybersecurity skills so that they can identify and mitigate the effects of cyber-attacks. Additionally, the findings support prior claims that cybersecurity awareness training is effective in increasing cybersecurity skills levels (Albrechtsen & Hovden, 2010; D'Arcy et al., 2009; Kritzinger & von Solms, 2010; Rahim et al., 2015). This study answered the calls from, and built upon work of several researchers who not only identified the cybersecurity skills that are needed by non-IT professionals, but also advocated the need for increasing the cybersecurity awareness and skills of Internet users, especially senior citizens to counter the effects of cyber-attacks (Carlton & Levy, 2015; D'Arcy et al., 2009; Grimes et al., 2010; Kritzinger & von Solms, 2010; Shillair et al., 2015).

The main goal of this research study was to empirically assess the contributions of senior citizens' cybersecurity awareness, computer self-efficacy, perceived risk of identity theft, and older adults' computer technology attitude on their motivation (intrinsic & extrinsic) to acquire cybersecurity skills, as well as their cybersecurity skill level, while comparing each before and after cybersecurity awareness training. From this main goal, six specific goals were developed, with each having a matching research question and proposition. The main research question that this study addressed was: what is the contribution of senior citizens' SCCA, CSE, PRIT, and OACTA on their motivation (IM & EM) to acquire cybersecurity skills, as well as their CyberSkills level,

while comparing it before and after cybersecurity awareness training? The seven propositions were:

P1_(a & b): There will be a significant positive contribution of senior citizens' SCCA on their (a) IM and (b) EM to acquire cybersecurity skills.

P2_(a & b): There will be a significant positive contribution of senior citizens' CSE on their (a) IM and (b) EM to acquire cybersecurity skills.

P3_(a & b): There will be a significant positive contribution of senior citizens' PRIT on their (a) IM and (b) EM to acquire cybersecurity skills.

P4_(a & b): There will be a significant positive contribution of senior citizens' OACTA on their (a) IM and (b) EM to acquire cybersecurity skills.

P5_(a & b): There will be a significant positive contribution of senior citizens' (a) IM and (b) EM to acquire cybersecurity skills on their CyberSkills level.

P6_(a & b): There will be significant mean difference in the levels of senior citizens' CyberSkills level before (t_1) and after (t_3) the cybersecurity awareness training.

P7_(a to h): There will be significant mean difference in the levels of senior citizens' CyberSkills level before (t_1) and after (t_3) the cybersecurity awareness training, when controlled for the following eight demographic indicators: (a) age, (b) gender, (c) years of using computers, (d) years of using the Internet, (e) years of using Internet-enabled mobile devices, (f) years of working in corporate or formal organization, (g) years since retiring, and (h) level of education.

After conducting a thorough literature review to establish the research problem, the methodology for this quantitative study that utilized a pre-experimental one group pretest-posttest design was outlined. The methodology followed a three-phased approach as follows. In phase one, the survey instrument was developed based on validated measures from prior research, and further validated using an expert-review process that followed the Delphi technique. The feedback from the expert panel finalized the survey instrument, which was then used in phase two in the pilot test. The survey instrument consisted of six sections and 64 items, with each section addressing each of the IVs.

In phase two, there was a pilot testing of the pre-and-post training measures using the survey instrument and the iPad app, namely MyCyberSkills™ iPad app. The iPad app consisted of scenarios that measured the DV. There were no changes to the survey instrument after the pilot test, however, some modifications were made to the main data collection procedures. The modifications increased participation as participants were no longer required to go to the computer lab for all stages of participation.

In phase three, the main data collection of the pre-and-post training measures that addressed the research questions, including data analysis, and interpretation was conducted. Using the Web-based survey instrument along with the Web-based iPad app, data was collected from 254 participants, ranging in age from 60 to 89, with a mean age of 70.24 years. At the end of the data collection period, which lasted for three months, pre-analysis data screening was conducted using SPSS. The descriptive statistics from SPSS confirmed that there were no missing values, all responses were within the specified ranges (minimum & maximum values), and the frequencies were valid. Outlier detection for the pre-and-post-tests was conducted using Mahalanobis Distance; some

UserID #s were identified as potential multivariate outliers and considered for elimination. However, after further analysis, including examining the stem-leaf graphs, the UserID #s were not significant and were not removed, thus all the responses from the 254 participants were kept. Path analysis in Smart PLS 3.0 addressed RQ1 to RQ4, as well as P1 to P5, ANOVA addressed RQ5 as well as P6, and ANCOVA addressed RQ6 and P7. The results from the analyses revealed some interesting and, in some cases, unexpected findings. Overall, two of the five propositions tested in Smart PLS 3.0 were fully supported in both the pre-and-post-tests. These included P2_(a & b), i.e. CSE → IM and CSE → EM, along with P3_(a & b), i.e. PRIT → IM and PRIT → EM. While the remaining propositions were not fully supported, none was rejected, as each was either fully supported in the pre-test and partially supported in the post-test, or vice-versa. For example, P1_(a) (SCCA → IM) was fully supported in the pre-test, but P1_(b) (SCCA → EM) was partially supported in the post-test. The two remaining propositions, i.e. P6_(a & b) and P7_(a to h) were tested in SPSS using ANOVA and ANCOVA. P6_(a & b) was supported and P7_(a to h) was mostly supported, with years using computers being the only demographic indicator that was found to be significant.

This study identified a number of limitations such as the generalization of the findings as the study did not consider factors such as culture, language, socio-economic conditions, and access to technology. Further, since there was an imbalance as it relates to the male/female ratio in the study. There was approximately only one quarter (25%) of the sample who were males, therefore, the findings may not be representative of male senior citizens in the general population. Another limitation relates to the scenarios that were included in the iPad app to test cybersecurity skills; they were more suited for

persons who were still in the workforce, and since over 50% of the participants have retired for more than five years, many of them found it difficult to relate to the scenarios. Other shortcomings in the iPad app that may have affected the scores were that some scenarios were split over more than one window, and some participants did not retain what was indicated in the previous window, plus there were no options to go back. In such cases, participants randomly clicked on answers. In other cases, the images and screen shots that were included in some scenarios were difficult to read, therefore, in such cases, again, the participants randomly chose answers. Both the survey questions and the iPad app scenarios were very lengthy (took on average 90 minutes in total to complete), and some participants became tired towards the end and did not pay much attention to the answers that they selected.

Ideas for future research were also presented in this study. Future research can continue to explore the factors that will motivate senior citizens to acquire cybersecurity skills so that they can adequately protect themselves from cyber-attacks. Future research can also consider developing a shorter cybersecurity assessment tool with scenarios that are more relevant to retirees and/or persons who are outside of the organizational context. After the development of such assessment tool, this study can be repeated to see if similar results will be seen. Future research could also develop and validate a cybersecurity awareness instrument for use within the HCU context, especially since cybersecurity awareness is now applicable to all Internet users.

Theoretically, this study adds to the body of knowledge on the factors that motivate senior citizens to acquire cybersecurity skills so that they will be empowered to mitigate the effects of cyber-attacks when the attacks occur. The study also adds to the

body of knowledge as it used SDT as the theoretical lens; SDT is not widely used in the InfoSec domain. The results of this study can also be valuable in assisting other researchers who attempt to investigate cybersecurity awareness within the context of older adults or senior citizens as the data was actually collected from a wide cross-section of participants whose demographics is representative of such populations. Practical implications of this study include developing the training content into a blue-print training model that can be administered to HCUs across the globe. Additionally, both the training content and the MyCyberSkills™ iPad app can be used together to address as well as assess cybersecurity issues among Internet users, regardless of context or age group. A “Train the Trainer” model was also recommended where more adept senior citizens can be trained to conduct the training. This should increase the reception and participation from the other senior citizens as the training would be conducted by one of their peers who better understands the challenges that are unique to them. Further, the recommendations along with the training content can be useful to law enforcement and other agencies that work with senior citizens in their efforts to address and reduce the number of reported cases relating to cybersecurity issues amongst senior citizens.

In conclusion, most prior studies focused on using the Internet and the benefits that senior citizens can get when they learn to use the Internet. This study is one of the few that focused on the dangers/threats that senior citizens face when they use the Internet and the skills that are required to counter the dangers/threats. As studies of this nature gain traction in the InfoSec domain, researchers will find unexpected results, and this may result in stronger associations between research in the fields of InfoSec and Gerontology to make better sense of the findings and how to solve potential problems.

Hence, in spite of the low R^2 values and weak relationships among the constructs that were observed in the assessed models, the findings from this study indicate that both intrinsic and extrinsic motivation, along with antecedents such as SCCA, CSE, PRIT, and OACTA significantly impact the cybersecurity skill levels of senior citizens. The low R^2 values and weak construct relationships also suggest that other factors than intrinsic and extrinsic motivation also impact the cybersecurity skills levels of senior citizens, and require further investigation. Finally, cybersecurity awareness training was found to be effective in increasing the cybersecurity skill levels of senior citizens, and hence empower them with the requisite skills to take mitigating actions against cyber-attacks. This should, therefore, reduce the success of cyber-attack vectors due to limited cybersecurity awareness and skills among senior citizens, which ultimately causes them significant financial losses.

Appendix A

Institutional Review Board Approval Letter



I

MEMORANDUM

To: **Carlene G Blackwood-Brown, BSc. and MSc.**

From: **Ling Wang, Ph.D.,
Center Representative, Institutional Review Board**

Date: **August 4, 2017**

Re: **IRB #: 2017-486; Title, "An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under 45 CFR 46.101(b) (Exempt Category 2). You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: **Yair Levy, Ph.D.
Ling Wang, Ph.D.**

Appendix B

Survey Instrument for Participants

Cybersecurity Awareness and Older Adults Survey

Dear Participant,

Thank you for agreeing to participate in this research. Please review the instructions and questions in each section below. The survey is divided into six sections, please see each of the sections below. You are being asked to complete all questions in each section, and then (optionally) provide your feedback on the overall survey instrument via the qualitative questions at the end.

After completing the survey, please select the ‘Submit’ button to save your responses. In the on-screen acknowledgement window that appears after you click the ‘Submit’ button, please click on the link that is provided to start the online cybersecurity skills assessment, or close the window if you would like to do the skills assessment at a later date.

Thank you again for your time and assistance.

Regards,

Carlene Blackwood-Brown, Ph.D. Candidate
E-mail: cb2136@mynsu.nova.edu

* Required

Identification

Please enter the ID# that was emailed to you: *

Your answer

Section 1. Cybersecurity Awareness (CSA)

The items in Section 1 below are related to how aware you are of some common cybersecurity threats that you may face when you are online. Please select from the dropdown list for each question to rate your level of awareness on each question from “1” to “7”, with “1” indicating “Not at all Aware” and “7” indicating “Extremely Aware”.

CSA1 - How aware are you of computer virus attacks? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA2 - How aware are you of identity theft resulting from phishing scams? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA3 - How aware are you of unauthorized people intercepting (i.e. capturing and stealing) your sensitive information online? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA4 - How aware are you of password security, e.g. setting strong passwords and keeping passwords safe? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA5 - How aware are you of computer security updates? *

Choose

- 1 - Not at all aware

- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA6 - How aware are you of the security of online copyrighted content (such as music or movies)? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA7 - How aware are you of social engineering attacks? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA8 - How aware are you of ransomware attacks? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

Section 2. Computer Self-Efficacy (CSE)

The items in Section 2 below are related to how you perceive your ability to use the computer. Please select from the dropdown list for each question to indicate your level of agreement on each question from “1” to “7”, with “1” indicating “Strongly Disagree” and “7” indicating “Strongly Agree.”

CSE1 - I am comfortable working with computers. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

CSE2 - I can learn to use most computer programs, if I am given some training. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

CSE3 - I can learn to use most computer programs just by reading the manuals and help documentations. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

Section 3. Risk of Identity Theft (PRIT)

The items in Section 3 below are related to your belief in the possibility that another person will unlawfully use your personally identifiable information (PII) for his/her personal gain. PII refers to information that can be used to identify or locate you, for example, name, address, phone number, email address, fax number, credit card number or Social Security Number. Please select from the dropdown list for each question to indicate your level of agreement on each question from “1” to “7”, with “1” indicating “Strongly Disagree” and “7” indicating “Strongly Agree.”

PerR1 - If my identity gets stolen while using the Internet, it would likely be because the Internet did not work properly. *

Choose

- 1 - Strongly disagree

- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PerR2 - If my identity gets stolen while using the Internet, it would likely be because the Internet did not work as well as I expected. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PerR3 - If my identity gets stolen while using the Internet, it would likely be because the Internet had technical problems. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PerR4 - If my identity gets stolen while using the Internet, it would likely be because I was not careful and made mistakes while using it. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SecR1 - If my identity gets stolen while using the Internet, it would likely be because the Internet is not secure. *

Choose

- 1 - Strongly disagree

- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SecR2 - If my identity gets stolen while using the Internet, it would likely be because fake websites are shown online. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SecR3 - If my identity gets stolen while using the Internet, it would likely be because the Internet may be attacked or hacked into. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

FinR1 - If my identity gets stolen while using the Internet, it is likely that I will lose money. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

FinR2 - If my identity gets stolen while using the Internet, it is likely that I will lose control of my bank account. *

Choose

- 1 - Strongly disagree

- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

FinR3 - If my identity gets stolen while using the Internet, it is likely that my money loss will not be covered by the bank. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PriR1 - If my identity gets stolen while using the Internet, it is likely that others will know my personal details. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PriR2 - If my identity gets stolen while using the Internet, it is likely that others will misuse my data. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PriR3 - If my identity gets stolen while using the Internet, it is likely that I will lose control of my personal data. *

Choose

- 1 - Strongly disagree

- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

TimR1 - If my identity gets stolen while using the Internet, it is likely that I will have to spend extra time solving problems that the identity theft caused. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

TimR2 - If my identity gets stolen while using the Internet, it is likely that I will not be as efficient as I was when I did not use the Internet. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PsyR1 - If my identity gets stolen while using the Internet, it is likely that I will feel frustrated. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PsyR2 - If my identity gets stolen while using the Internet, it is likely that I will feel anxious. *

Choose

- 1 - Strongly disagree

- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PsyR3 - If my identity gets stolen while using the Internet, it is likely that I will feel depressed. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SocR1 - If my identity gets stolen while using the Internet, it is likely that I will look foolish to others. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SocR2 - If my identity gets stolen while using the Internet, it is likely that my usage of the Internet will be judged negatively by others. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SocR3 - If my identity gets stolen while using the Internet, it is likely that my decision to use the Internet will not be socially accepted by others. *

Choose

- 1 - Strongly disagree

- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PhyR1 - If my identity gets stolen while using the Internet, it is likely that I will have a headache. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PhyR2 - If my identity gets stolen while using the Internet, it is likely that my eyesight will be affected (e.g. get sore eyes). *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

Section 4. Computer Technology Attitude (OACTA)

The items in Section 4 below are related to your feelings or judgment about computer technology. Please select from the dropdown list for each question to indicate your level of agreement on each question from “1” to “7”, with “1” indicating “Strongly Disagree” and “7” indicating “Strongly Agree.”

CCVII - I do not like the idea of using the Internet as a way to communicate. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

CCVI2 - I believe that senior citizens have no use of the Internet. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

CCVI3 - I do not want to use the Internet because I much prefer human contact. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

CCVI4 - The Internet is only intended to be used by young and middle-age people. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

CCVI5 - I would rather write or telephone than send messages to people through the Internet. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SACT1 - I wish the computer/smart device screen was built to be easier to use by senior citizens. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SACT2 - I wish the computer/smart device keyboard was built to be easier to use by senior citizens. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SACT3 - I wish the computer/smart device mouse/touchscreen was built to be easier to use by senior citizens. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SACT4 - I would use the computer/smart device mouse/touchscreen if it was built to accommodate the needs of senior citizens. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PhyCCT1 - Computer/smart device screens are hard to read. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PhyCCT2 - To sit in front of a computer/smart device is uncomfortable. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PhyCCT3 - The computer/smart device mouse/touchscreen is hard to use. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PhyCCT4 - It is hard to type on the keyboard of a computer/smart device. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PsyCCT1 - I am not comfortable with the idea of using a computer/smart device. *

Choose

- 1 - Strongly disagree
- 2 - Disagree

- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PsyCCT2 - I do not believe that I would ever be able to learn how to properly use a computer/smart device. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PsyCCT3 - Computers/smart devices make me feel left behind technologically. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PsyCCT4 - I do not feel comfortable with the idea of 'surfing the net' (like looking up information on different topics on the Internet). *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

Section 5. Interest in Cybersecurity Training

The items in Section 5 below are related to what drives or inspires you to acquire cybersecurity skills. Please select from the dropdown list for each question to indicate how each question reflects you from "1" to "7", with "1" indicating "Very Untrue of Me" and "7" indicating "Very True of Me."

IM1 - In a cybersecurity training course, I would prefer material that really challenges me so I can learn new things. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

IM2 - In a cybersecurity training course, I would prefer material that arouses my curiosity, even if it is difficult to learn. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

IM3 - In a cybersecurity training course, the most satisfying thing for me would be to try to understand the content as thoroughly as possible. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

IM4 - In a cybersecurity training course, if given the opportunity, I would choose course tasks that I can learn from even if they don't guarantee a good score. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

EM1 - In a cybersecurity training course, getting a good score would be the most satisfying thing for me. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

EM2 - In a cybersecurity training course, the most important thing for me would be improving my overall score average, so my main concern would be getting a good score.

*

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

EM3 - In a cybersecurity training course, if I could, I would want to get better scores than most of the other students. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

EM4 - In a cybersecurity training course, I would want to do well because it is important to show my ability to my family, friends, or others. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

Section 6. Demographic Information

The items in Section 6 below are related to demographics about our survey participants. Please tell us a little more about yourself.

D1. What is your gender? *

Choose

- 1) Female
- 2) Male

D2. What is your age group? *

Choose

- 1) 64 or under
- 2) 65 to 69
- 3) 70 to 74
- 4) 75 to 79
- 5) 80 to 84
- 6) 85 to 89
- 7) 90 or over

D3. How many years have you been using computers? *

Choose

- 1) 5 to 9
- 2) 10 to 14
- 3) 15 to 19
- 4) 20 to 24
- 5) 25 to 29
- 6) 30 to 34
- 7) 35 or over

D4. How many years have you been using the Internet? *

Choose

- 1) 5 to 9
- 2) 10 to 14
- 3) 15 to 19
- 4) 20 to 24
- 5) 25 to 29
- 6) 30 to 34
- 7) 35 or over

D5. How many years have you been using Internet-enabled devices, e.g. smartphone, laptop, tablet/iPad)? *

Choose

- 1) 1 to 4
- 2) 5 to 9
- 3) 10 to 14
- 4) 15 to 19
- 5) 20 to 24
- 6) 25 to 29
- 7) 30 or over

D6. How many years have you worked in a corporate or formal organization? *

Choose

- 1) 1 to 4
- 2) 5 to 9
- 3) 10 to 14
- 4) 15 to 19
- 5) 20 to 24
- 6) 25 to 29
- 7) 30 or over

D7. How many years has it been since you retired? *

Choose

- 1) 0 to 4
- 2) 5 to 9
- 3) 10 to 14
- 4) 15 to 19
- 5) 20 to 24
- 6) 25 to 29
- 7) 30 or over

D8. What is your highest level of education? *

Choose

- 1) High School graduate/GED
- 2) Some college
- 3) Associate's degree
- 4) Bachelor's degree
- 5) Master's degree
- 6) Doctoral degree
- 7) Professional degree

Qualitative Questions about the Survey Instrument (Optional)

Please give your feedback on the survey instrument - this section is optional.

QPT-1a: After reading through the survey instrument, are the user directions to complete each section clear and understandable?

Yes

No

QPT-1b: If NO, please explain and offer recommendations:

Your answer

QPT-2a: Is each question stated in a clear and understandable manner?

Yes

No

QPT-2b: If NO, please explain and offer recommendations:

Your answer

QPT-3a: Is the scale for the questions clear and understandable?

Yes

No

QPT-3b: If NO, please explain and offer recommendations:

Your answer

QPT-4a: Are there any questions you would recommend deleting?

Yes

No

QPT-4b: If YES, please explain and offer recommendations:

Your answer

QPT-5a: Are there any questions you would recommend adding?

Yes

No

QPT-5b: If YES, please explain and offer recommendations:

Your answer

QPT-6a: Are there any other revisions to the questions or scales in this survey instrument that you would recommend?

Yes

No

QPT-6b: If YES, please explain and offer recommendations:

Your answer

Submit

Appendix C

Expert Panel Recruitment Email

Dear Information Systems and Cybersecurity Expert,

I am kindly requesting your volunteer participation as a member of an expert panel to provide anonymous feedback on a survey instrument for my doctoral research study. Based on your expertise you were identified as someone who could provide expert and qualitative evaluation of the instrument.

My name is Carlene Blackwood-Brown and I am a Ph.D. candidate in Information Systems at the College of Engineering and Computing, Nova Southeastern University, working under the supervision of Professor Yair Levy, and a member of his Levy CyLab (<http://CyLab.nova.edu/>). My research will investigate the factors that would motivate senior citizens to acquire cybersecurity skills so that they can identify, as well as know how to mitigate against cyber-attacks. My dissertation title is: *An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills*. The factors that will be investigated are cybersecurity awareness, computer self-efficacy, perceived risk of identity theft, older adults' computer technology attitude, and motivation (intrinsic & extrinsic) to acquire cybersecurity skills. I, therefore, need your assistance in validating the items for each factor. The items were validated in prior research, however, this is the first time that they will all be used on the same instrument.

In the capacity as a member of the expert panel, I respectfully ask that you review a draft survey instrument and complete the qualitative evaluation immediately below each section of the survey. Your input will be incorporated into finalizing the instrument for the participants.

The information that you provide will be used for this research study and used in aggregated form. No personal identifiable information (PII) will be collected, and all your feedback will be completely anonymous. As a member of the expert panel, you agree to keep all information regarding this research confidential and to refrain from disclosing any details related to this survey or the material contained within it. Please be advised that this research is under process with the NSU's Cybersecurity Incubator, and as such, full confidentiality is required.

If you are willing to participate in this phase of the research, maintain a high level of confidentiality, and non-disclosure as it pertains items, *please reply to this email within five (5) days of receiving it*. After accepting, a follow-up email with the link to the draft

survey and corresponding qualitative evaluation will be sent to you. If you prefer the email with the link to be sent to an alternate email address, please provide it with your reply. If you wish to decline, please reply indicating that.

Thank you in advance for your time and consideration. I appreciate your assistance and contribution to this research study. Should you wish to receive the findings of the study, please indicate such with your reply email and I will be happy to provide you with information about the academic research publication(s) resulting from this study.

Regards,

Carlene Blackwood-Brown, Ph.D. Candidate
E-mail: cb2136@nova.edu

Appendix D

Expert Panel Questionnaire with Instrument

Dear Information Systems and Cybersecurity Expert,

Thank you for agreeing to participate on the expert panel for this draft survey instrument. I am a Ph.D. candidate in Information Systems at the College of Engineering and Computing, Nova Southeastern University, working under the supervision of Professor Yair Levy, and a member of his Levy CyLab (<http://CyLab.nova.edu/>). My research will investigate the factors that would motivate senior citizens to acquire cybersecurity skills so that they can identify, as well as know how to mitigate against cyber-attacks. My dissertation title is: An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills. The factors that will be investigated are cybersecurity awareness, computer self-efficacy, perceived risk of identity theft, older adults' computer technology attitude, and motivation (intrinsic & extrinsic) to acquire cybersecurity skills.

Please note that in order to reduce response bias, the names of three of the factors to be investigated have been renamed on the instrument: Perceived Risk of Identity Theft has been renamed Risk of Identity Theft; Older Adults' Computer Technology Attitude has been renamed Computer Technology Attitude; and Motivation (intrinsic & extrinsic) to Acquire Cybersecurity Skills has been renamed Interest in Cybersecurity Training.

Please review the instructions and items in each section below, and offer your feedback via the corresponding qualitative questions below each section. Each section is represented as an image and the qualitative questions that you are required to answer are below each image. I respectfully ask that you complete the evaluation within five days of receipt of this correspondence. It should take no more than 20 minutes to complete.

After completing the evaluation, please select the 'Submit' button to save and submit your anonymous responses.

Thank you again for your time and assistance.

Regards,
Carlene Blackwood-Brown, Ph.D. Candidate
E-mail: cb2136@mynsu.nova.edu

* Required

Section 1. Cybersecurity Awareness (CSA)

Section 1. Cybersecurity Awareness

The items in Section 1 below are related to how aware you are of some common cybersecurity threats that you may face when you are online. Cybersecurity awareness involves “alerting Internet users of cybersecurity issues and threats, and enhancing Internet users’ understanding of cyber threats so they can be fully committed to embracing security during Internet use”. (Adapted from Kajzer, D’Arcy, Crowell, Striegel, & Brügger, 2014).

Please respond to the following items by rating your level of awareness on each item from “1” to “7”, with “1” indicating “Not at all Aware” and “7” indicating “Extremely Aware”. Please make one selection per row.

	Item	1 Not at all aware	2 Low awareness	3 Slightly aware	4 Neither aware nor unaware	5 Moderately aware	6 Very aware	7 Extremel y aware
CSA1	Computer virus attacks	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
CSA2	Identity theft resulting from phishing scam	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
CSA3	Unauthorized people intercepting your sensitive information online	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
CSA4	Password security	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
CSA5	Computer security updates	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
CSA6	Online copyrighted content (such as music or movies)	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>

Expert Panel Qualitative Questions for Section 1 - please answer these questions.

S1-1a: After reading through Section 1, are the user directions to complete this section of the survey instrument clear and understandable? *

Yes

No

S1-1b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

◀
▶

◀
▶

S1-2a: Is each item stated in a clear and understandable manner? *

Yes

No

S1-2b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S1-3a: Is the scale for the items clear and understandable? *

Yes

No

S1-3b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S1-4a: Do the items appropriately measure the Cybersecurity Awareness construct? *

Yes

No

S1-4b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S1-5a: Are there any items you would recommend deleting? *

Yes

No

S1-5b: If YES, please explain and offer recommendations. If No, please enter NA: *

S1-6a: Are there any items you would recommend adding? *

Yes

No

S1-6b: If YES, please explain and offer recommendations. If No, please enter NA: *

S1-7a: Are there any other revisions to Section 1 – Cybersecurity Awareness items or scales that you would recommend? *

Yes

No

S1-7b: If YES, please explain and offer recommendations. If No, please enter NA: *

S1-8: Please offer any other comments or recommendations that would help improve validity or reliability. Please enter NA if nothing to add. *

Section 2. Computer Self-Efficacy (CSE)

Section 2. Computer Self-Efficacy

The items in Section 2 below are related to how you perceive your ability to use the computer. Computer Self-Efficacy is “an individual’s perceptions of his or her ability to use computers in the accomplishment of a task”. (Adapted from Compeau & Higgins, 1995, as well as Bhatnagar, Madden, & Levy, 2016).

Please respond to the following items by rating your level of agreement on each item from “1” to “7”, with “1” indicating “Strongly Disagree” and “7” indicating “Strongly Agree.” Please make one selection per row.

	Item	1 Strongly disagree	2 Disagree	3 Somewhat disagree	4 Neither agree nor disagree	5 Somewhat agree	6 Agree	7 Strongly agree
CSE1	I am comfortable working with computers	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
CSE2	I can learn to use most computer programs, if I am given some training	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
CSE3	I can learn to use most computer programs just by reading the manuals and help documentations	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>

Expert Panel Qualitative Questions for Section 2 - please answer these questions.

S2-1a: After reading through Section 2, are the user directions to complete this section of the survey instrument clear and understandable? *

Yes

No

S2-1b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S2-2a: Is each item stated in a clear and understandable manner? *

Yes

No

S2-2b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S2-3a: Is the scale for the items clear and understandable? *

Yes

No

S2-3b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S2-4a: Do the items appropriately measure the Computer Self-Efficacy construct? *

Yes

No

S2-4b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S2-5a: Are there any items you would recommend deleting? *

Yes

No

S2-5b: If YES, please explain and offer recommendations. If No, please enter NA: *

S2-6a: Are there any items you would recommend adding? *

Yes

No

S2-6b: If YES, please explain and offer recommendations. If No, please enter NA: *

S2-7a: Are there any other revisions to Section 2 – Computer Self-Efficacy items or scales that you would recommend? *

Yes

No

S2-7b: If YES, please explain and offer recommendations. If No, please enter NA: *

S2-8: Please offer any other comments or recommendations that would help improve validity or reliability. Please enter NA if nothing to add. *

Section 3. Risk of Identity Theft (PRIT)

Section 3. Risk of Identity Theft

The items in Section 3 below are related to your belief in the possibility that another person will unlawfully use your personally identifiable information (PII) for his/her personal gain while you are online. PII refers to information that can be used to identify or locate you, for example, name, address, phone number, email address, fax number, credit card number or Social Security Number. There are eight different dimensions of risk that is used in this study; each is defined below. (Adapted from Zhao, Hanmer-Lloyd, Ward, & Goode, 2008).

Please respond to the following items by rating your level of agreement on each item from “1” to “7”, with “1” indicating “Strongly Disagree” and “7” indicating “Strongly Agree.” Please make one selection per row.

	Item	1 Strongly disagree	2 Disagree	3 Somewhat disagree	4 Neither agree nor disagree	5 Somewhat agree	6 Agree	7 Strongly agree
Performance Risk (PerR) – this refers to your perception that your identity may get stolen because the Internet may malfunction and not work properly when you use it.								
PerR1	If my identity gets stolen while using the Internet, it would likely be because the Internet did not work properly.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PerR2	If my identity gets stolen while using the Internet, it would likely be because the Internet will not work as well as I expected.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PerR3	If my identity gets stolen while using the Internet, it would likely be because the Internet has technical problems.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PerR4	If my identity gets stolen while using the Internet, it would likely be because I was not careful and made mistakes while using it.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
Security Risk (SecR) – this refers to concerns you may have regarding the potential loss that can result from using networks that do not have adequate security which can result in fraudulent activities by cyber-criminals, e.g. stealing your identity.								

	Item	1 Strongly disagree	2 Disagree	3 Somewhat disagree	4 Neither agree nor disagree	5 Somewhat agree	6 Agree	7 Strongly agree
SecR1	If my identity gets stolen while using the Internet, it would likely be because the Internet is not secure.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
SecR2	If my identity gets stolen while using the Internet, it would likely be because fake websites are shown online.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
SecR3	If my identity gets stolen while using the Internet, it would likely be because the Internet may be attacked or hacked into.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
Financial Risk (FinR) – this refers to your perception that your identity will be stolen while using the Internet, and hence, you will suffer financial loss.								
FinR1	If my identity gets stolen while using the Internet, it is likely that I will lose money	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
FinR2	If my identity gets stolen while using the Internet, it is likely that I will lose control of my bank account	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
FinR3	If my identity gets stolen while using the Internet, it is likely that my money loss will not be covered by the bank.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
Privacy Risk (PriR) – this refers to your perception of the loss of privacy and confidentiality of your PII which can result in identity theft online.								
PriR1	If my identity gets stolen while using the Internet, it is likely that others	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>

	Item	1 Strongly disagree	2 Disagree	3 Somewhat disagree	4 Neither agree nor disagree	5 Somewhat agree	6 Agree	7 Strongly agree
	will know my personal details							
PriR2	If my identity gets stolen while using the Internet, it is likely that others will misuse my data	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PriR3	If my identity gets stolen while using the Internet, it is likely that I will lose control of my personal data	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
Time Risk (TimR) – this refers to your perception of any loss of time you may incur because of having to expend extra effort to learn how to protect yourself from identity theft, and to resolve any issues that may arise if your identity gets stolen while using the Internet.								
TimR1	If my identity gets stolen while using the Internet, it is likely that I will have to spend extra time solving problems that the identity theft caused	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
TimR2	If my identity gets stolen while using the Internet, it is likely that I will not be as efficient as I was when I did not use the Internet	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
Psychological Risk (PsyR) – this refer to your perception that you will suffer mental stress or not have peace of mind when you use the Internet for fear of being a victim of identity theft.								
PsyR1	If my identity gets stolen while using the Internet, it is likely that I will feel frustrated	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PsyR2	If my identity gets stolen while using the Internet, it is likely that I will feel anxious	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PsyR3	If my identity gets stolen while using the Internet, it is	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>

S3-2a: Is each item stated in a clear and understandable manner? *

Yes

No

S3-2b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S3-3a: Is the text explaining each subcategory of Risk clear, understandable, and helpful? *

*

Yes

No

S3-3b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S3-4a: Is the scale for the items clear and understandable? *

Yes

No

S3-4b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S3-5a: Do the items appropriately measure the Risk of Identity Theft construct? *

Yes

No

S3-5b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S3-6a: Are there any items you would recommend deleting? *

Yes

No

S3-6b: If YES, please explain and offer recommendations. If No, please enter NA: *

S3-7a: Are there any items you would recommend adding? *

Yes

No

S3-7b: If YES, please explain and offer recommendations. If No, please enter NA: *

S3-8a: 8. Are there any other revisions to Section 3 – Risk of Identity Theft items or scales that you would recommend? *

Yes

No

S3-8b: If YES, please explain and offer recommendations. If No, please enter NA: *

S3-9: Please offer any other comments or recommendations that would help improve validity or reliability. Please enter NA if nothing to add. *

Section 4. Computer Technology Attitude (OACTA)

Section 4. Computer Technology Attitude

The items in Section 4 below are related to your feelings or judgment about computer technology. Computer Technology Attitude refers to an "individual's general assessment or feeling towards specific computer and Internet related activities". (Adapted from Laganá, Oliver, Ainsworth, & Edwards, 2011).

Please respond to the following items by rating your level of agreement on each item from "1" to "7", with "1" indicating "Strongly Disagree" and "7" indicating "Strongly Agree." Please make one selection per row.

	Item	1 Strongly disagree	2 Disagree	3 Somewhat disagree	4 Neither agree nor disagree	5 Somewhat agree	6 Agree	7 Strongly agree
Comfort Communicating via Internet (CCVI) – this refers to how comfortable you are using the Internet as a means of communication.								
CCVI1	I do not like the idea of using the Internet as a way to communicate	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
CCVI2	I believe that the elderly has no use for the Internet	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
CCVI3	I do not want to use the Internet because I much prefer human contact	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
CCVI4	The Internet is only intended to be used by young and middle-age people	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
CCVI5	I would rather write or telephone than send messages to people through the Internet	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
Satisfaction with Available Computer Technology (SACT) - this refers to your satisfaction with the computer technology that is available to you.								
SACT1	I wish a computer screen were built to be easier to use by older adults than it is now	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
SACT2	I wish a computer keyboard were built to be easier to use by older	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>

	Item	1 Strongly disagree	2 Disagree	3 Somewhat disagree	4 Neither agree nor disagree	5 Somewhat agree	6 Agree	7 Strongly agree
	adults than it is now							
SACT3	I wish a computer mouse were built to be easier to use by older adults than it is now	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
SACT4	I would use a computer mouse if it were built to accommodate the needs of older adults	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
Physical Comfort with Computer Technology (PhyCCT)								
PhyCCT 1	Computer screens are hard to read	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PhyCCT 2	To sit in front of a computer is uncomfortable	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PhyCCT 3	The computer mouse is hard to use	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PhyCCT 4	It is hard to type on the keyboard of a computer	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
Psychological Comfort with Computer Technology (PsyCCT)								
PsyCCT 1	I am not comfortable with the idea of using a computer	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PsyCCT 2	I do not believe that I would ever be able to learn how to properly use a computer	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PsyCCT 3	Computers make me feel left behind technologically	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
PsyCCT 4	I do not feel comfortable with the idea of 'surfing the net' (like looking up information on different topics on the Internet)	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>

Expert Panel Qualitative Questions for Section 4 - please answer these questions.

S4-1a: After reading through Section 4, are the user directions to complete this section of the survey instrument clear and understandable? *

Yes

No

S4-1b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S4-2a: Is each item stated in a clear and understandable manner? *

Yes

No

S4-2b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S4-3a: Is the text explaining each subcategory of Computer Technology Attitude clear, understandable, and helpful?

Yes

No

S4-3b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S4-4a: Is the scale for the items clear and understandable? *

Yes

No

S4-4b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S4-5a: Do the items appropriately measure the Computer Technology Attitude construct?

*

Yes

No

S4-5b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

An empty rectangular text input box with a light gray border. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom, both with standard arrow and track icons.

S4-6a: Are there any items you would recommend deleting? *

Yes

No

S4-6b: If YES, please explain and offer recommendations. If No, please enter NA: *

An empty rectangular text input box with a light gray border. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom, both with standard arrow and track icons.

S4-7a: Are there any items you would recommend adding? *

Yes

No

S4-7b: If YES, please explain and offer recommendations. If No, please enter NA: *

An empty rectangular text input box with a light gray border. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom, both with standard arrow and track icons.

S4-8a: Are there any other revisions to Section 4 – Computer Technology Attitude items or scales that you would recommend? *

Yes

No

S4-8b: If YES, please explain and offer recommendations. If No, please enter NA: *

An empty rectangular text input box with a light gray border. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom, both with standard arrow and track icons.

S4-9: Please offer any other comments or recommendations that would help improve validity or reliability. Please enter NA if nothing to add. *

An empty rectangular text input box with a light gray border. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom, both with standard arrow and track icons.

Section 5. Interest in Cybersecurity Training

Section 5. Interest in Cybersecurity Training

The items in Section 5 below are related to what drives or inspires you to acquire cybersecurity skills. An interested or inspired person is someone who is energized and enthused to perform an activity. (Adapted from Nausheen, 2016 as well as Pintrich, Smith, Garcia, & McKeachie, 1993).

Please respond to the following items by rating how each item reflects you from “1” to “7”, with “1” indicating “Very Untrue of Me” and “7” indicating “Very True of Me.” Please make one selection per row.

	Item	1 Very untrue of me	2 Untrue of me	3 Somewhat untrue of me	4 Neutral	5 Somewhat true of me	6 True of me	7 Very true of me
IM1	In a cybersecurity training course, I prefer material that really challenges me so I can learn new things	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
IM2	In a cybersecurity training course, I prefer material that arouses my curiosity, even if it is difficult to learn.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
IM3	The most satisfying thing for me in a cybersecurity training course is trying to understand the content as thoroughly as possible.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
IM4	When I have the opportunity in a cybersecurity training course, I choose course tasks that I can learn from even if they don't guarantee a good score.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
EM1	Getting a good score in a cybersecurity training course is the most satisfying thing for me right now.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
EM2	The most important thing for me right now is improving my overall score average, so my main concern in a cybersecurity training course is getting a good score.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
EM3	If I can, I want to get better scores in a cybersecurity training course than most of the other students.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>
EM4	I want to do well in a cybersecurity training course because it is important to show my ability to my family, friends, or others.	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>

Expert Panel Qualitative Questions for Section 5 - please answer these questions.

S5-1a: After reading through Section 5, are the user directions to complete this section of the survey instrument clear and understandable? *

Yes

No

S5-1b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S5-2a: Is each item stated in a clear and understandable manner? *

Yes

No

S5-2b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S5-3a: Is the scale for the items clear and understandable? *

Yes

No

S5-3b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S5-4a: Do the items appropriately measure the Interest in Cybersecurity Training construct? *

Yes

No

S5-4b: If NO, please explain and offer recommendations. If Yes, please enter NA: *

S5-5a: Are there any items you would recommend deleting? *

Yes

No

S5-5b: If YES, please explain and offer recommendations. If No, please enter NA: *

S5-6a: Are there any items you would recommend adding? *

Yes

No

S5-6b: If YES, please explain and offer recommendations. If No, please enter NA: *

S5-7a: Are there any other revisions to Section 5 – Interest in Cybersecurity Training items or scales that you would recommend? *

Yes

No

S5-7b: If YES, please explain and offer recommendations. If No, please enter NA: *

S5-8: Please offer any other comments or recommendations that would help improve validity or reliability. Please enter NA if nothing to add. *

Section 6. Demographic Information (to be completed by expert panel member)

The items in Section 6 below are related to demographics about yourselves as members of the expert panel. Please answer all questions.

D1. What is your gender? *

1) Female

2) Male

D2. What is your age group? *

1) Under 18

2) 18 to 24

3) 25 to 29

4) 30 to 39

5) 40 to 49

6) 50 to 59

7) 60 or over

D3. How many years have you been working in the field of information security/cybersecurity? *

- 1) Under 5
- 2) 5 to 9
- 3) 10 to 14
- 4) 15 to 19
- 5) 20 to 24
- 6) 25 to 29
- 7) 30 or over

D4. Do you have any information security/cybersecurity certification? *

- 1) Yes
- 2) No

D5. What is your highest level of education? *

- 1) High School graduate/GED
- 2) Some college
- 3) Associate's degree
- 4) Bachelor's degree
- 5) Master's degree
- 6) Doctoral degree
- 7) Professional certification

Appendix E

Pilot Test Solicitation Letter

Dear Pilot Test Participant,

My name is Carlene Blackwood-Brown and I am a Ph.D. candidate in Information Systems at the College of Engineering and Computing, Nova Southeastern University, working under the supervision of Professor Yair Levy, and a member of his Levy CyLab (<http://CyLab.nova.edu/>). My dissertation title is: *An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills*.

I am kindly requesting your volunteer participation in a pilot test for my research. Your participation will be three-fold: completing an online survey with a qualitative evaluation, completing an online cybersecurity skills assessment, and attending a face-to-face cybersecurity awareness training session. Specifically,

1. You will be required to complete a set of questions via an online survey. The survey is divided into six sections and should take approximately 45 minutes to an hour to complete. I will respectfully ask that you review the survey items, provide an answer to each, and then complete the qualitative evaluation immediately below each section. This will be done to solicit your feedback on the clarity of the survey items and scales, as well as any other recommendations you may have to improve the survey before it is distributed to hundreds of other senior citizens. Therefore, your feedback is very important. Please note that you will be required to complete the survey at two different times, before the cybersecurity awareness training, as well as after the training.
2. You will be required to complete an online cybersecurity skills assessment. The assessment will take about one hour to complete. Please note that you will be required to complete the assessment at two different times, before the cybersecurity awareness training, as well as after the training.
3. You will be required to attend a face-to-face cybersecurity awareness training session. This will take place at a location near you and should last for about two hours. The date and time will be communicated to you in a timely manner. The training will be done only once.

In order to participate, you should meet the following requirements: be 65 years or older, and have been accessing the Internet via an Internet-enabled mobile device (smartphone, tablet/iPad, laptop, etc.) for at least one year. As a participant, the following applies:

- Your identity, survey responses, and assessment scores will be kept anonymous
- No personally identifiable information will be collected from you
- The information that you provide in the survey will be completely anonymous
- The data that will be collected will only be published in aggregated form, and used only for academic purposes

- Your participation in this survey is voluntary and, you may exit (i.e., opt-out) of the survey at any time.

As a pilot test participant, you agree to keep all information regarding this research confidential and to refrain from disclosing any details related to this survey or the material contained within it.

If you are willing to participate in this phase of the research, maintain a high level of confidentiality, and non-disclosure as it pertains items, *please reply to this email within five days of receiving it*. After accepting, a follow-up email with the next steps will be sent to you. If you wish to decline, please reply indicating that.

Thank you in advance for your time and consideration. I appreciate your assistance and contribution to this research study.

Regards,

Carlene Blackwood-Brown, Ph.D. Candidate
E-mail: cb2136@nova.edu

Appendix F

Pilot Test Questionnaire with Instrument

Cybersecurity Awareness and Older Adults Survey

Dear Pilot Test Participant,

Thank you for agreeing to participate in this research. Please review the instructions and questions in each section below. The survey is divided into six sections, please see each of the sections below. You are being asked to complete all questions in each section, and then (optionally) provide your feedback on the overall survey instrument via the qualitative questions at the end.

After completing the survey, please select the ‘Submit’ button to save your responses. In the on-screen acknowledgement window that appears after you click the ‘Submit’ button, please click on the link that is provided to start the online cybersecurity skills assessment, or close the window if you would like to do the skills assessment at a later date.

Thank you again for your time and assistance.

Regards,

Carlene Blackwood-Brown, Ph.D. Candidate
E-mail: cb2136@mynsu.nova.edu

* Required

Identification

Please enter the ID# that was emailed to you: *

Your answer

Section 1. Cybersecurity Awareness (CSA)

The items in Section 1 below are related to how aware you are of some common cybersecurity threats that you may face when you are online. Please select from the dropdown list for each question to rate your level of awareness on each question from “1” to “7”, with “1” indicating “Not at all Aware” and “7” indicating “Extremely Aware”.

CSA1 - How aware are you of computer virus attacks? *

Choose

1 - Not at all aware

2 - Low awareness

- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA2 - How aware are you of identity theft resulting from phishing scams? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA3 - How aware are you of unauthorized people intercepting (i.e. capturing and stealing) your sensitive information online? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA4 - How aware are you of password security, e.g. setting strong passwords and keeping passwords safe? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA5 - How aware are you of computer security updates? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware

- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA6 - How aware are you of the security of online copyrighted content (such as music or movies)? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA7 - How aware are you of social engineering attacks? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

CSA8 - How aware are you of ransomware attacks? *

Choose

- 1 - Not at all aware
- 2 - Low awareness
- 3 - Slightly aware
- 4 - Neither aware nor aware
- 5 - Moderately aware
- 6 - Very aware
- 7 - Extremely aware

Section 2. Computer Self-Efficacy (CSE)

The items in Section 2 below are related to how you perceive your ability to use the computer. Please select from the dropdown list for each question to indicate your level of agreement on each question from “1” to “7”, with “1” indicating “Strongly Disagree” and “7” indicating “Strongly Agree.”

CSE1 - I am comfortable working with computers. *

Choose

- 1 - Strongly disagree

- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

CSE2 - I can learn to use most computer programs, if I am given some training. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

CSE3 - I can learn to use most computer programs just by reading the manuals and help documentations. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

Section 3. Risk of Identity Theft (PRIT)

The items in Section 3 below are related to your belief in the possibility that another person will unlawfully use your personally identifiable information (PII) for his/her personal gain. PII refers to information that can be used to identify or locate you, for example, name, address, phone number, email address, fax number, credit card number or Social Security Number. Please select from the dropdown list for each question to indicate your level of agreement on each question from “1” to “7”, with “1” indicating “Strongly Disagree” and “7” indicating “Strongly Agree.”

PerR1 - If my identity gets stolen while using the Internet, it would likely be because the Internet did not work properly. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree

- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PerR2 - If my identity gets stolen while using the Internet, it would likely be because the Internet did not work as well as I expected. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PerR3 - If my identity gets stolen while using the Internet, it would likely be because the Internet had technical problems. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PerR4 - If my identity gets stolen while using the Internet, it would likely be because I was not careful and made mistakes while using it. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SecR1 - If my identity gets stolen while using the Internet, it would likely be because the Internet is not secure. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

SecR2 - If my identity gets stolen while using the Internet, it would likely be because fake websites are shown online. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

SecR3 - If my identity gets stolen while using the Internet, it would likely be because the Internet may be attacked or hacked into. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

FinR1 - If my identity gets stolen while using the Internet, it is likely that I will lose money. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

FinR2 - If my identity gets stolen while using the Internet, it is likely that I will lose control of my bank account. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

FinR3 - If my identity gets stolen while using the Internet, it is likely that my money loss will not be covered by the bank. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PriR1 - If my identity gets stolen while using the Internet, it is likely that others will know my personal details. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PriR2 - If my identity gets stolen while using the Internet, it is likely that others will misuse my data. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PriR3 - If my identity gets stolen while using the Internet, it is likely that I will lose control of my personal data. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

TimR1 - If my identity gets stolen while using the Internet, it is likely that I will have to spend extra time solving problems that the identity theft caused. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

TimR2 - If my identity gets stolen while using the Internet, it is likely that I will not be as efficient as I was when I did not use the Internet. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

PsyR1 - If my identity gets stolen while using the Internet, it is likely that I will feel frustrated. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

PsyR2 - If my identity gets stolen while using the Internet, it is likely that I will feel anxious. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

PsyR3 - If my identity gets stolen while using the Internet, it is likely that I will feel depressed. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

SocR1 - If my identity gets stolen while using the Internet, it is likely that I will look foolish to others. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

SocR2 - If my identity gets stolen while using the Internet, it is likely that my usage of the Internet will be judged negatively by others. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

SocR3 - If my identity gets stolen while using the Internet, it is likely that my decision to use the Internet will not be socially accepted by others. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

PhyR1 - If my identity gets stolen while using the Internet, it is likely that I will have a headache. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

PhyR2 - If my identity gets stolen while using the Internet, it is likely that my eyesight will be affected (e.g. get sore eyes). *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

Section 4. Computer Technology Attitude (OACTA)

The items in Section 4 below are related to your feelings or judgment about computer technology. Please select from the dropdown list for each question to indicate your level of agreement on each question from “1” to “7”, with “1” indicating “Strongly Disagree” and “7” indicating “Strongly Agree.”

CCVII - I do not like the idea of using the Internet as a way to communicate. *

Choose

1 - Strongly disagree

2 - Disagree

3 - Somewhat disagree

4 - Neither agree nor disagree

5 - Somewhat agree

6 - Agree

7 - Strongly agree

CCVII2 - I believe that senior citizens have no use of the Internet. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

CCVI3 - I do not want to use the Internet because I much prefer human contact. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

CCVI4 - The Internet is only intended to be used by young and middle-age people. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

CCVI5 - I would rather write or telephone than send messages to people through the Internet. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SACT1 - I wish the computer/smart device screen was built to be easier to use by senior citizens. *

Choose

- 1 - Strongly disagree
- 2 - Disagree

- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SACT2 - I wish the computer/smart device keyboard was built to be easier to use by senior citizens. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SACT3 - I wish the computer/smart device mouse/touchscreen was built to be easier to use by senior citizens. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

SACT4 - I would use the computer/smart device mouse/touchscreen if it was built to accommodate the needs of senior citizens. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PhyCCT1 - Computer/smart device screens are hard to read. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree

- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PhyCCT2 - To sit in front of a computer/smart device is uncomfortable. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PhyCCT3 - The computer/smart device mouse/touchscreen is hard to use. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PhyCCT4 - It is hard to type on the keyboard of a computer/smart device. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PsyCCT1 - I am not comfortable with the idea of using a computer/smart device. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PsyCCT2 - I do not believe that I would ever be able to learn how to properly use a computer/smart device. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PsyCCT3 - Computers/smart devices make me feel left behind technologically. *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

PsyCCT4 - I do not feel comfortable with the idea of 'surfing the net' (like looking up information on different topics on the Internet). *

Choose

- 1 - Strongly disagree
- 2 - Disagree
- 3 - Somewhat disagree
- 4 - Neither agree nor disagree
- 5 - Somewhat agree
- 6 - Agree
- 7 - Strongly agree

Section 5. Interest in Cybersecurity Training

The items in Section 5 below are related to what drives or inspires you to acquire cybersecurity skills. Please select from the dropdown list for each question to indicate how each question reflects you from "1" to "7", with "1" indicating "Very Untrue of Me" and "7" indicating "Very True of Me."

IM1 - In a cybersecurity training course, I would prefer material that really challenges me so I can learn new things. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me

- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

IM2 - In a cybersecurity training course, I would prefer material that arouses my curiosity, even if it is difficult to learn. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

IM3 - In a cybersecurity training course, the most satisfying thing for me would be to try to understand the content as thoroughly as possible. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

IM4 - In a cybersecurity training course, if given the opportunity, I would choose course tasks that I can learn from even if they don't guarantee a good score. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

EM1 - In a cybersecurity training course, getting a good score would be the most satisfying thing for me. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me

- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

EM2 - In a cybersecurity training course, the most important thing for me would be improving my overall score average, so my main concern would be getting a good score.

*

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

EM3 - In a cybersecurity training course, if I could, I would want to get better scores than most of the other students. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

EM4 - In a cybersecurity training course, I would want to do well because it is important to show my ability to my family, friends, or others. *

Choose

- 1 - Very untrue of me
- 2 - Untrue of me
- 3 - Somewhat untrue of me
- 4 - Neutral
- 5 - Somewhat true of me
- 6 - True of me
- 7 - Very true of me

Section 6. Demographic Information

The items in Section 6 below are related to demographics about our survey participants. Please tell us a little more about yourself.

D1. What is your gender? *

Choose

1) Female

2) Male

D2. What is your age group? *

Choose

1) 64 or under

2) 65 to 69

3) 70 to 74

4) 75 to 79

5) 80 to 84

6) 85 to 89

7) 90 or over

D3. How many years have you been using computers? *

Choose

1) 5 to 9

2) 10 to 14

3) 15 to 19

4) 20 to 24

5) 25 to 29

6) 30 to 34

7) 35 or over

D4. How many years have you been using the Internet? *

Choose

1) 5 to 9

2) 10 to 14

3) 15 to 19

4) 20 to 24

5) 25 to 29

6) 30 to 34

7) 35 or over

D5. How many years have you been using Internet-enabled devices, e.g. smartphone, laptop, tablet/iPad)? *

Choose

1) 1 to 4

2) 5 to 9

3) 10 to 14

4) 15 to 19

5) 20 to 24

6) 25 to 29

7) 30 or over

D6. How many years have you worked in a corporate or formal organization? *

Choose

1) 1 to 4

2) 5 to 9

3) 10 to 14

4) 15 to 19

5) 20 to 24

6) 25 to 29

7) 30 or over

D7. How many years has it been since you retired? *

Choose

1) 0 to 4

2) 5 to 9

3) 10 to 14

4) 15 to 19

5) 20 to 24

6) 25 to 29

7) 30 or over

D8. What is your highest level of education? *

Choose

1) High School graduate/GED

2) Some college

3) Associate's degree

4) Bachelor's degree

5) Master's degree

6) Doctoral degree

7) Professional degree

Qualitative Questions about the Survey Instrument (Optional)

Please give your feedback on the survey instrument - this section is optional.

QPT-1a: After reading through the survey instrument, are the user directions to complete each section clear and understandable?

Yes

No

QPT-1b: If NO, please explain and offer recommendations:

Your answer

QPT-2a: Is each question stated in a clear and understandable manner?

Yes

No

QPT-2b: If NO, please explain and offer recommendations:

Your answer

QPT-3a: Is the scale for the questions clear and understandable?

Yes

No

QPT-3b: If NO, please explain and offer recommendations:

Your answer

QPT-4a: Are there any questions you would recommend deleting?

Yes

No

QPT-4b: If YES, please explain and offer recommendations:

Your answer

QPT-5a: Are there any questions you would recommend adding?

Yes

No

QPT-5b: If YES, please explain and offer recommendations:

Your answer

QPT-6a: Are there any other revisions to the questions or scales in this survey instrument that you would recommend?

Yes

No

QPT-6b: If YES, please explain and offer recommendations:

Your answer

Submit

Appendix G

Participant Email

General Instructions

Dear research participant,

Thank you for your time and willingness to participate in this survey and online cybersecurity skills assessment.

My name is Carlene Blackwood-Brown and I am a Ph.D. candidate at Nova Southeastern University in Florida, where I am conducting research for my dissertation. The research will primarily investigate the factors that would motivate senior citizens to acquire cybersecurity skills so that they can identify, as well as know how to mitigate against cyber-attacks. My doctoral advisor is Dr. Yair Levy, Professor of Information Systems and Cybersecurity in the School of Engineering and Computing at Nova Southeastern University. My dissertation title is: *An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills*.

In order to participate, you should meet the following requirements: be 65 years or older, and have been accessing the Internet via an Internet-enabled mobile device (smartphone, tablet/iPad, laptop, etc.) for at least one year. As a research participant, the following applies:

- Your identity, survey responses, and assessment scores will be kept anonymous
- No personally identifiable information will be collected from you
- The information that you provide in the survey will be completely anonymous
- The data that will be collected will only be published in aggregated form, and used only for academic purposes
- Your participation in this survey is voluntary and, you may exit (i.e., opt-out) of the survey at any time.

Your participation in this research is three-fold: completing an online survey, completing an online cybersecurity skills assessment, and attending a face-to-face cybersecurity awareness training session. Specifically,

1. You will be required to complete a set of questions via an online survey. The survey is divided into six sections and should take approximately 25-30 minutes to complete. Please ensure that you answer all questions as you will not be able to submit the survey until all the questions are answered. When all the questions are answered, please ensure that you click the "Submit" button to record your participation in the survey. When the survey submission is complete, you will receive an on-screen acknowledgement. Please note that you will be required to

complete the survey at two different times, before the cybersecurity awareness training, as well as after the training.

2. You will be required to complete an online cybersecurity skills assessment. In the on-screen acknowledgement window that you receive after submitting the survey, please click on the provided link and follow the instructions to start the online cybersecurity skills assessment. The assessment will take about one hour to complete. Please note that you will be required to complete the assessment at two different times, before the cybersecurity awareness training, as well as after the training.
3. You will be required to attend a face-to-face cybersecurity awareness training session. This will take place at a location near you and should last for about two hours. The date and time will be communicated to you in a timely manner. The training will be done only once.

If you have any questions, you can contact me via cb2136@nova.edu.

Again, thank you for your time and participation in this research.

Sincerely,

Carlene Blackwood-Brown, Ph.D. Candidate
Nova Southeastern University

References

- Abawajy, J. (2014). User preference of cybersecurity awareness delivery methods. *Behavior & Information Technology*, 33(3), 236-247.
- Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker, J. F. (2010). Detecting fake websites: The contribution of statistical learning theory. *MIS Quarterly*, 34(3), 435-461.
- Abedalaziz, N., Jamaluddin, S., & Chin, H. L. E. N. G. (2013). Measuring attitudes toward computer and internet usage among postgraduate students in Malaysia. *TOJET: The Turkish Online Journal of Educational Technology*, 12(2), 200-216.
- Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*, 5(1), 5-14.
- Akopyan, D. A., & Yelyakov, A. D. (2009). Cybercrimes in the information structure of society: A survey. *Scientific and Technical Information Processing*, 36(6), 338-350.
- Aïmeur, E., & Schonfeld, D. (2011). The ultimate invasion of privacy: Identity theft. *Proceedings of the 2011 Ninth Annual International Conference on Privacy, Security and Trust (PST)*, Montreal, Canada, pp. 24-31.
- Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29(4), 432-445.
- Aldás-Manzano, J., Lassala-Navarré, C., Ruiz-Mafé, C., & Sanz-Blas, S. (2009). The role of consumer innovativeness and perceived risk in online banking usage. *The International Journal of Bank Marketing*, 27(1), 53-75.
- Anderson, K. B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing*, 25(2), 160-171.
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613-A15.

- Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal of Economic Perspectives*, 22(2), 171-192.
- Ansley, J. & Erber, J. T. (1988). Computer interaction: Effect on attitudes and performance in older adults. *Educational Gerontology*, 14(2), 107-119.
- Anti-Phishing Working Group (2015). Phishing activity trends report, 4th quarter 2014. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf
- Bandura, A. (1986). *Social foundation of thought and action: A social cognitive theory*. Englewood Cliffs, NJ: Prentice Hall.
- Bellah, J. (2001). Training: Identity theft. *Law & Order*, 49(10), 222-227.
- Bettman, J. R. (1973). Perceived risk and its components: A model and empirical test. *Journal of Marketing Research*, 10(2), 184-190.
- Bhatnagar, N., Madden, H., & Levy, Y. (2016). Initial empirical testing of potential factors contributing to patient use of secure medical teleconferencing. *The Journal of Computer Information Systems*, 57(1), 89-95.
- Boss, S. R., Galletta, D. F., Benjamin Lowry, P., 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.
- Boss, S., Kirsch, L., Angermeier, I., Shingler, R., & Boss, R. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151-164.
- Boudreau, M., D. Gefen, & D. Straub (2001). Validation in IS research: A state-of-the-art assessment. *MIS Quarterly*, 25(1), 1-23.
- Boyatzis, R. E., & Kolb, D. A. (1991). Assessing individuality in learning: The learning skills profile. *Educational Psychology*, 11(3/4), 279-295.
- Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, Law and Social Change*, 46(4-5), 189-206.
- Brewer, N. T., Chapman, G. B., Gibbons, F. X., Gerrard, M., McCaul, K. D., & Weinstein, N. D. (2007). Meta-analysis of the relationship between risk perception and health behavior: The example of vaccination. *Health Psychology*, 26(2), 136-145.

- Broadly, T., Chan, A., & Caputi, P. (2010). Comparison of older and younger adults' attitudes towards and abilities with computers: Implications for training and learning. *British Journal of Educational Technology*, 41(3), 473-485.
- Budhrani, R., & Sridaran, R. (2014). Wireless local area networks: Threats and their discovery using WLANs scanning tools. *International Journal of Advanced Networking & Applications (IJANA)*, 137-150.
- 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-A7.
- Campbell, M. C., & Goodstein, R. C. (2001). The moderating effect of perceived risk on consumers' evaluations of product incongruity: Preference for the norm. *Journal of Consumer Research*, 28(3), 439-449.
- Carlton, M. (2016). *Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (UMI No. 10240271).
- Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. *Proceedings of the 2015 IEEE SoutheastCon*, Ft. Lauderdale, Florida, pp.1-6.
- Carvalho, S. W., Block, L. G., Sivaramakrishnan, S., Manchanda, R. V., & Mitakakis, C. (2008). Risk perception and risk avoidance: The role of cultural identity and personal relevance. *International Journal of Research in Marketing*, 25(4), 319-326.
- Cassidy, S., & Eachus, P. (2002). Development of the computer user self-efficacy (CUSE) Scale: Investigating the relationship between computer self-efficacy, gender and experience with computers. *Journal of Educational Computing Research*, 26(2), 169-89.
- Chen, K., & Chan, A. H. (2013). Use or non-use of gerontechnology - A qualitative study. *International Journal of Environmental Research and Public Health*, 10(10), 4645-4666.
- Choi, M. S. (2013). *Assessing the role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills toward computer misuses intention at government agencies* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (UMI No. 3599848).

- Choo, K-K. R. (2008). Organized crime groups in cyberspace: A typology. *Trends in Organized Crime, 11*(3), 270-295.
- Choo, K-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.
- Choo, K-K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organized crime groups. *Asian Journal of Criminology, 3*(1), 37-59.
- Chris Zhao, Y., & Zhu, Q. (2014). Effects of extrinsic and intrinsic motivation on participation in crowdsourcing contest. *Online Information Review, 38*(7), 896-917.
- Cicchetti, D. V., Shoinralter, D., & Tyrer, P. J. (1985). The effect of number of rating scale categories on levels of interrater reliability: A Monte Carlo investigation. *Applied Psychological Measurement, 9*(1), 31-36.
- Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems, 52*(4), 20-29.
- Cody, M. J., Dunn, D., Hoppin, S., & Wendt, P. (1999). Silver surfers: Training and evaluating internet use among older adult learners. *Communication Education, 48*(4), 269-286.
- Compeau, D., & Higgins, C. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-211.
- Compeau, D., Marcolin, B., Kelley, H., & Higgins, C. (2012). Generalizability of information systems research using student subjects – a reflection of our practices and recommendations for future research. *Information Systems Research, 23*(4), 1093-1109.
- Cota, T. T., Ishitani, L., & Vieira Jr. N. (2015). Mobile game design for the elderly: A study with focus on the motivation to play. *Computers in Human Behavior, 51*(A), 96-105.
- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21.
- Creswell, J. W. (2002). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Upper Saddle River, New Jersey: Merrill Prentice Hall.
- Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (2nd ed.). Upper Saddle River, NJ: Pearson.

- Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research, 4th Edition*. Boston, MA: Pearson Education Inc.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches, 4th Edition*. Thousand Oaks, CA: Sage Publication.
- Czaja, S. J., & Sharit, J. (1998). Age differences in attitudes toward computers. *Journal of Gerontology: Psychological Sciences, 53B*(5), 329-340.
- Dane, F. C. (2011). *Evaluating research, 1st Edition*. Thousand Oaks, CA: Sage Publications.
- Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies, 72*(2), 154-168.
- D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*(1), 59-71.
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.
- Deci, E. L. (1971). Effects of externally mediated rewards on intrinsic motivation. *Journal of Personality and Social Psychology, 18*(1), 105-115.
- Deci, E. L., & Ryan, R. M. (1985). *Intrinsic motivation and self-determination in human behavior*. New York: Plenum.
- Delbecq, A. L., Ven, A. H. V. d., & Gustafson, D. (1975). *Group techniques for program planning: A guide to nominal group and Delphi process*. Glenview, IL: Scott Foresman.
- Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295-316.
- Dowling, G. R. (1986). Perceived risk: The concept and its measurement. *Psychology & Marketing, 3*(3), 193-210.
- Eisma, R., Dickinson, A., Goodman, J., Syme, A., Tiwari, L., & Newell, A. F. (2004). Early user involvement in the development of information technology-related

- products for older people. *Universal Access in the Information Society*, 3(2), 131-140.
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, 6, 323-337.
- Ellis, T. J., & Levy, Y. (2010). A guide for novice researchers: Design and development research methods. *Proceedings of Informing Science & IT Education Conference, InSITE*.
- Fan, W., & Yan, Z. (2010). Factors affecting response rates of the web survey: A systematic review. *Computers in Human Behavior*, 26, 132-139.
- Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451-474.
- Featherman, M. S., & Wells, J. D. (2010). The intangibility of e-services: Effects on perceived risk and acceptance. *Database for Advances in Information Systems*, 41(2), 110-131.
- Federal Trade Commission. (2000). *Privacy online: Fair information practices in the electronic marketplace: A report to Congress*. Washington: The Commission. Retrieved from <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>
- Feng, X., Fu, S., & Qin, J. (2016). Determinants of consumers' attitudes toward mobile advertising: The mediating roles of intrinsic and extrinsic motivations. *Computers in Human Behavior*, 63, 334-341.
- Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security*, 2008(4), 6-9.
- Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, 26(5), 410-417.
- Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security*, 27(7-8), 235-240.
- Futcher, A. L. L. (2015). A framework to assist email users in the identification of phishing attacks. *Information & Computer Security*, 23(4), 1-14.
- Gabel, M. J., & Shipan, C. R. (2004). A social choice approach to expert consensus panels. *Journal of Health Economics*, 23(3), 543-564.

- Gatto, S. L., & Tak, S. H. (2008). Computer, Internet, and e-mail use among older adults: Benefits and barriers. *Educational Gerontology, 34*(9), 800-811.
- 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*(5), 91-109.
- Gefen, D., Straub, D. W., & Boudreau, M. (2000). Structural equation modeling techniques and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*(7), 1-79.
- Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 24*(1), 16-30.
- Gist, M. E. (1987). Self-efficacy: Implications for organizational behavior and human resource management. *The Academy of Management Review, 12*(3), 472-485.
- Goodwin, C. L. (2013). Use of the computer and the Internet by well older adults. *Activities, Adaptation & Aging, 37*(1), 63-78.
- Greengard, S. (2009). Facing an age-old problem. *Communications of the Association of Computing Machinery, 52*(9), 20-22.
- Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of Internet hazards. *Educational Gerontology, 36*(3), 173-192.
- Hair, J. F., Hult, J. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: Sage Publication.
- Hall, M. T., & Marshall, J. E. (2016). Intrinsic and extrinsic motivation within the context of modern education. In E. Railean, G. Walker, A. Elçi, & L. Jackson (Eds.), *Handbook of research on applied learning theory and design in modern education* (pp. 292-308). Hershey, PA: IGI Global.
- Hanafizadeh, P., & Khedmatgozar, H. R. (2012). The mediating role of the dimensions of the perceived risk in the effect of customers' awareness on the adoption of Internet banking in Iran. *Electronic Commerce Research, 12*(2), 151-175.
- Hart, C. (1998). *Doing a literature review: Releasing the social science research imagination*. London, UK: Sage Publications.
- Hart, T. A., Chaparro, B. S., & Halcomb, C. G. (2008). Evaluating websites for older adults: adherence to 'senior-friendly' guidelines and end-user performance. *Behavior & Information Technology, 27*(3), 191-199.

- Hasan, B., & Ali, J. M. H. (2004). An empirical examination of a model of computer learning performance. *The Journal of Computer Information Systems*, 44(4), 27-33.
- Hayashi, A., Chen, C., Ryan, T., & Wu, J. (2004). The role of social presence and moderating role of computer self-efficacy in predicting the continuance usage of E-learning systems. *Journal of Information Systems Education*, 15(2), 139-154.
- Henson, B., Reynolds, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice*, 29(4), 475-497.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2), 106-125.
- Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets on-line: Products and market forces. *Criminal Justice Studies* 23(1), 33–50.
- Holt, J., & Turner, G. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior*, 33(4), 308–323.
- Hong, J. (2012). The state of phishing attacks. *Communications of the Association for Computing Machinery*, 55(1), 74-81.
- Igbaria, M., & Iivari, J. (1995). The effects of self-efficacy on computer usage. *Omega*, 23(6), 587-605.
- Im, I., Kim, Y., & Han, H. (2008). The effects of perceived risk and technology type on users' acceptance of technologies. *Information & Management*, 45(1), 1-9.
- Imgraben, J., Engelbrecht, A., & Choo, K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, 33(12), 1347-1360.
- Inan, F. A., Namin, A. S., Pogrund, R. L., & Jones, K. S. (2016). Internet use and cybersecurity concerns of individuals with visual impairments. *Journal of Educational Technology & Society*, 19(1), 28-40.
- Iyer, R., & Eastman, J. K. (2006). The elderly and their attitudes toward the Internet: The impact on Internet use, purchase, and comparison shopping. *Journal of Marketing Theory and Practice*, 14(1), 57-67.

- Jacoby, J., & Kaplan, L. B. (1972). The components of perceived risk. *Proceedings of the 3rd Annual Conference of the Association for Consumer Research*, 382-393.
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993.
- Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behavior & Information Technology*, 32(6), 584-593.
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-A4.
- Jones, T. L. (2001). Protecting the elderly. *Law & Order*, 49(4), 102-106.
- Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? *The Journal of Computer Information Systems*, 53(2), 22-30.
- Karsten, R., Mitra, A., & Schmidt, D. (2012). Computer self-efficacy: A meta-analysis. *Journal of Organizational and End User Computing*, 24(4), 54-80.
- Kelley, C. L., & Chames, N. (1995). Issues in training older adults to use computers. *Behavior and Information Technology*. 14(2), 107-120.
- Kher, H. V., Downey, J. P., & Monk, E. (2013). A longitudinal examination of computer self-efficacy change trajectories during training. *Computers in Human Behavior*, 29(4), 1816-1824.
- Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, 22(1), 115-126.
- Kritzinger, E., & von Solms, S. H. (2010). Cybersecurity for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), 840-847.
- Kruger, H. A., & Kearney, W. D. (2008). Consensus ranking - An ICT security awareness case study. *Computers & Security*, 27(7-8), 254-259.
- Kumar, K., & Kadhiravan, S. (2012). Perceived stress and proactive coping of college students. *Indian Journal of Positive Psychology*, 3(3), 302-304.
- Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, 46(1), 254-264.

- Laganá, L., & García, J. J. (2013). The mental health impact of computer and Internet training on a multi-ethnic sample of community-dwelling older adults: Results of a pilot randomized controlled trial. *International Journal of Biomedical Science*, 9(3), 135-147.
- Laganá, L., Oliver, T., Ainsworth, A., & Edwards, M. (2011). Enhancing computer self-efficacy and attitudes in multi-ethnic older adults: A randomized controlled study. *Ageing and Society*, 31(6), 911-933.
- Lai, F. Li, D., & Hsieh, C-T. (2012). Fighting identity theft: The coping perspective, *Decision Support Systems*, 52(2), 353-363.
- Lam, J. C., & Lee, M. O. (2006). Digital inclusiveness - Longitudinal study of Internet adoption by older adults. *Journal of Management Information Systems*, 22(4), 177-206.
- Lee, M. K. O., Cheung, C. M. K., & Chen, Z. (2005). Acceptance of Internet-based learning medium: The role of extrinsic and intrinsic motivation. *Information & Management*, 42(8), 1095-1104.
- Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177-187.
- Lee, Y., Lee, J., & Hwang, Y. (2015). Relating motivation to information and communication technology acceptance: Self-determination theory perspective. *Computers in Human Behavior*, 51(Part A), 418-428.
- Leedy, P. D., & Ormrod, J. E. (2005). *Practical research: Planning and design* (8th Ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
- Lemoudden, M., Bouazza, N. B., El Ouahidi, B., & Bourget, D. (2013). A survey of cloud computing security overview of attack vectors and defense mechanisms. *Journal of Theoretical & Applied Information Technology*, 54(2), 325-330.
- Lepper, M. R., Corpus, J. H., & Iyengar, S. S. (2005). Intrinsic and extrinsic motivational orientations in the classroom: Age differences and academic correlates. *Journal of Educational Psychology*, 97(2), 184-196.
- Lerouge, C., Newton, S., & J, E. B. (2005). Exploring the systems analyst skill set: Perceptions, preferences, age, and gender. *The Journal of Computer Information Systems*, 45(3), 12-23.
- Levine, T., & Donitsa-Schmidt, S. (1998). Computer use, confidence, attitudes, and knowledge: A causal analysis. *Computers in Human Behavior*, 14(1), 125-146.

- Levy, Y. (2005). A case study of management skills comparison in online MBA programs. *International Journal of Information and Communication Technology Education*, 1(3), 1-20.
- Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science Publishing.
- Levy, Y., & Danet, T. (2010). Implementation success model in Government agencies: A case of a centralized identification system at NASA. *International Journal of Information Systems in the Service Sector*, 2(2), 19-32.
- Levy, Y., Ramim, M. M., & Hackney, R. A. (2013). Assessing ethical severity of e-learning systems security attacks. *The Journal of Computer Information Systems*, 53(3), 75-84.
- Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.
- Liao, C., Lin, H., & Liu, Y. (2010). Predicting the use of pirated software: A contingency model integrating perceived risk with the theory of planned behavior. *Journal of Business Ethics*, 91(2), 237-252.
- Liaw, S. S. (2002). Understanding user perceptions of World Wide Web environments. *Journal of Computer Assisted Learning*, 18(2), 137-148.
- Lin, Y., McKeachie, W. J., & Kim, Y. C. (2002). College student intrinsic and/or extrinsic motivation and learning. *Learning and Individual Differences*, 13(3), 215-258.
- Loyd, B. H. & Loyd, D. E. (1985). The reliability and validity of instruments for the assessment of computer attitudes. *Educational and Psychological Measurement*, 45(4), 903-908.
- Lu, H-P., Hsu, C-L., & Hsu, H-Y. (2005). An empirical study of the effect of perceived risk upon intention to use online applications. *Information Management & Computer Security*, 13(2), 106-120.
- Maddison, J., & Jeske, D. (2014). Fear and perceived likelihood of victimization in traditional and cyber settings. *International Journal of Cyber Behavior, Psychology and Learning (IJCBL)*, 4(4), 23-40.

- Maditinos, D., Chatzoudes, D., & Sarigiannidis, L. (2013). An examination of the critical factors affecting consumer acceptance of online banking. *Journal of Systems and Information Technology*, 15(1), 97-116.
- Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.
- Marakas, G. M., Johnson, R. D., & Clay, P. F. (2007). The evolving nature of the computer self-efficacy construct: An empirical investigation of measurement construction, validity, reliability and stability over time. *Journal of the Association for Information Systems*, 8(1), 15-46.
- Marakas, G., Yi, M., & Johnson, R. (1998). The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research. *Information Systems Research*, 9(2), 126-164.
- Marquié, J. C., Jourdan-Boddaert, L., & Huet, N. (2002). Do older adults underestimate their actual computer knowledge? *Behaviour & Information Technology*, 21(4), 273-280.
- Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, 50(4), 370-396.
- Mattord, H. J., Levy, Y., & Furnell, S. (2013). An expert panel approach on developing a unified system authentication benchmarking index. *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)*, 5(2), 32-42.
- McAfee Inc. (2014). *Net Losses: Estimating the global cost of cybercrime: Economic impact of cybercrime II*. Santa Clara, CA: Center for Strategic and International Studies. Retrieved from <http://www.mcafee.com/tw/resources/reports/rp-economic-impact-cybercrime2.pdf>
- McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, 9(1), 23-41.
- Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal*, 14(2), 91-116.
- Mertler, C., & Vannatta, R. A. (2013). *Advanced and multivariate statistical methods*. Glendale, CA: Pyrczak Publishing.

- Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6), 2366-2375.
- Moon, J. W., & Kim, Y. G. (2001). Extending TAM for a World Wide Web context. *Information and Management*, 38(4), 21-23.
- Morgan, J., & Ravindran, S. (2014). An examination of home Internet and mobile device use in the U.S. *Interdisciplinary Journal of Information, Knowledge & Management*, 9, 1-18.
- Morris, R. (2010). Identity thieves and levels of sophistication: Findings from a national probability sample of American newspaper articles 1995-2005. *Deviant Behavior* 31(2), 184-207.
- Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus*, 140(4), 70-92.
- Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). Exploring game design for cybersecurity training. *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, Bangkok, 2012, pp. 256-262.
- National Initiative for Cybersecurity Careers and Studies (NICCS). (2015). *Cybersecurity 101*. Retrieved from <https://niccs.us-cert.gov/awareness/cybersecurity-101>
- National Institute of Standards and Technology (NIST). (2011, March). *Managing information security risk organization, mission, and information system view*. Retrieved from <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>
- Nemati, H. R., & Van Dyke, T. (2009). Do privacy statements really work? The effect of privacy statements and fair information practices on trust and perceived risk in E-commerce. *International Journal of Information Security and Privacy*, 3(1), 45-64.
- Ng, C. (2007). Motivation among older adults in learning computing technologies: A grounded model. *Educational Gerontology*, 34(1), 1-14.
- Noor, M. M., & Hassan, W. H. (2013). Wireless networks: Developments, threats and countermeasures. *International Journal of Digital Information and Wireless Communications (IJDIWC)*, 3(1), 119-134.

- Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management*, 42(1), 15-29.
- Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity strategy's role in raising Kenyan awareness of mobile security threats. *Information & Security*, 32(2), 1-20.
- Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, 43(4), 626-642.
- Paine, C., Reips, U., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet user's perceptions of privacy concerns and privacy actions. *International Journal of Human-Computer Studies*, 65(6), 526-536.
- Peltier, T. R. (2005). Implementing an information security awareness program. *Information Systems Security*, 14(2), 37-48.
- Perrin, P., & Duggan, M. (2015). *Americans' Internet Access: 2000-2015*. Pew Research Center. Retrieved from <http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/>
- Phipps, S. T. A., Prieto, L. C., & Ndinguri, E. N. (2013). Teaching an old dog new tricks: Investigating how age, ability, and self-efficacy influence intentions to learn and learning among participants in adult education. *Academy of Educational Leadership Journal*, 17(1), 13-25.
- Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. *Information Management & Computer Security*, 20(5), 382-420.
- Purkait, S., Kumar De, S., & Suar, D. (2014). An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. *Information Management & Computer Security*, 22(3), 194-234.
- Rahim, N. H. A., Hamid, S., Kiah, L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, 44(4), 606-622.
- Ramim, M. M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber-attacks and novice IT management in a small university. *Journal of Cases on Information Technology*, 8(4), 24-35.
- Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, 2(1), 122-136.

- Rea, L. M., & Parker, R. A. (2014). *Designing and conducting survey research: A comprehensive guide (4th Ed.)*. San Francisco, CA: Jossey-Bass.
- Regan, D. T., & Fazio, R. (1977). On the consistency between attitudes and behavior: Look to the method of attitude formation. *Journal of Experimental and Social Psychology, 13*(1), 28–45.
- Reisig, M., Pratt, T., & Holtfreter, K. (2009). Perceived risk of Internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior, 36*(4), 369-384.
- Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7-8), 241–253.
- Rhee, H., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.
- Richter, T., Naumann, J., & Groeben, N. (2000). Attitudes toward the computer: Construct validation of an instrument with scales differentiated by content. *Computers in Human Behavior, 16*(5), 473-491.
- Rigby, C. S., Deci, E. L., Patrick, B. C., & Ryan, R. M. (1992). Beyond the intrinsic-extrinsic dichotomy. *Motivation and Emotion, 16*(3), 165–185.
- Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyberidentity theft and related fraudulent activity. *Psychiatry, Psychology and Law, 20*(3), 315-328.
- Ryan, R. M., & Deci, E. L. (2000). Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary Educational Psychology, 25*(1), 54-67.
- Salkind, Neil J. (2012). *Exploring research, 8th Edition*. Upper Saddle River, NJ: Pearson Education Inc.
- Savona, E. U., & Mignone, M. (2004). The fox and the hunters: How IC technologies change the crime race. *European Journal on Criminal Policy and Research, 10*(1), 3-26.
- Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill-building approach, 6th Edition*. New York, NY: John Wiley & Sons Inc.
- Scheele, D. S. (1975). Reality construction as a product of Delphi interaction. In H. A. Linstone, & M. Turoff (Eds.), *The Delphi method: Techniques and applications* (pp. 37-71). Reading, MA: Addison-Wesley Publishing Company.

- Schmidt, L. I., Wahl, H., & Plischke, H., (2014). Older adults' performance in technology-based tasks: Cognitive ability and beyond. *Journal of Gerontological Nursing, 40*(4), 18-24.
- Schubert, R. (2006). Analyzing and managing risks - on the importance of gender differences in risk attitudes. *Managerial Finance, 32*(9), 706-715.
- Shapira, N., Barak, A., & Gal, I. (2007). Promoting older adults' well-being through Internet training and use. *Aging & Mental Health, 11*(5), 477-484.
- Shillair, R., Cotten, S. R., Tsai, H-Y. 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.
- Slegers, K., van Boxtel, M. P. J., & Jolles, J. (2012). Computer use in older adults: Determinants and the relationship with cognitive change over a 6 year episode. *Computers in Human Behavior, 28*(1), 1-10.
- Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy & Security, 8*(4), 3-26.
- Smith, B., Caputi, P., & Rawstone, L. (2000). Differentiating computer experience and attitude towards computers: An empirical investigation. *Computers in Human Behavior, 16*(1), 59-81.
- Stalker, J. D. (2012). *A reading preference and risk taxonomy for printed proprietary information compromise in the aerospace and defense industry* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (UMI No. 3548930).
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.
- Straub, D., Boudreau, M., & Gefen, D. (2004). Validation guidelines for is positivist research. *Communications of the Association for Information Systems, 13*(1), 380-427.
- Symantec Corporation. (2013). *2013 Norton Report*. Retrieved from http://www.symantec.com/en/ca/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013
- Symantec Corporation. (2014). *Internet security threat report 2014* (Vol. 19). Symantec Corporation. Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2014.pdf

- Tabachnick, B. G., & Fidell, L. S. (2007). *Using Multivariate Statistics, Fifth edition*. Boston, MA: Pearson/Allyn and Bacon.
- Teo, T. S-H., Lim, V. K. G., & Lai, R. Y. C. (1999). Intrinsic and extrinsic motivation in Internet usage. *Omega*, 27(1), 25-37.
- Terrell, S. (2012). *Statistics translated: A step-by-step guide to analyzing and interpreting data*. New York, NY: The Guilford Press.
- Torkzadeh, G., & Lee, J. (2003). Measures of perceived end-user computing skills. *Information & Management*, 40(7), 607-615.
- Tsai, H-Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138-150.
- Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective*, 17(5/6), 207-227.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science*, 46(2), 186-204.
- von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38(1), 97-102.
- Wagner, N., Hassanein, K., & Head, M. (2010). Computer use by older adults: A multi-disciplinary review. *Computers in Human Behavior*, 26(5), 870-882.
- Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy & Security*, 9(4), 52-79.
- Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2), 13-23.
- Weigel, F. K., & Hazen, B. T. (2014). Technical proficiency for IS success. *Computers in Human Behavior*, 31, 27-36.
- 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, J. & Weatherall, A. (2000). A grounded theory analysis of older adults and information technology. *Educational Gerontology*, 26(4), 371-386.
- Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM*, 46(8), 91-95.
- Willis, D. P. (2015, June 15). 5 steps for seniors to avoid financial fraud. *McClatchy - Tribune Business News* Retrieved from <http://www.app.com/story/money/business/consumer/2015/06/15/senior-financial-fraud/71264182/>
- Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring an information security awareness program. *Review of Business Information Systems*, 15(3), 9-22.
- Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security*, 16(5), 463-483.
- 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.
- Yazdipour, R., & Neace, W. P. (2013). Operationalizing a behavioral finance risk model: A theoretical and empirical framework. *The Journal of Entrepreneurial Finance*, 16(2), 1-32.
- Zhang, Y., & Espinoza, S. (1998). Relationships among computer-self-efficacy, attitudes toward computers, and desirability of learning computer skills. *Journal of Research on Computing in Education*, 30(4), 420-438.
- Zikmund, W. G. (2013). *Business research methods, 9th Edition*. New York, NY: Dryden Press.