COMPARING SECURITY SELF-EFFICACY AMONGST COLLEGE FRESHMEN AND SENIOR, FEMALE AND MALE CYBERSECURITY STUDENTS

by

Lane H. Melton

Liberty University

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Education

Liberty University

July 26, 2019

COMPARING SECURITY SELF-EFFICACY AMONGST COLLEGE FRESHMEN AND SENIOR, FEMALE AND MALE CYBERSECURITY STUDENTS

by

Lane H. Melton

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Education

Liberty University, Lynchburg, VA

July 26, 2019

APPROVED BY:

Alan Wimberley, Ed.D., Committee Chair

Darren Wu, Ed.D., Committee Member

Gary Metts, Ph.D., Committee Member

ABSTRACT

This study sought to determine if there was a difference in the self-efficacy of freshman and senior, female and male Cybersecurity students relating to threats associated with various information systems. The design for this quantitative study was non-experimental, causal-comparative and known as group comparison used to determine if there was a causal relationship between variables. The method used to make that determination utilized a self-efficacy survey developed by Phelps (2005), to identify the independent variables specific level of self-efficacy. Research was conducted at a small, southern university with total of 33 participants. Each student was enrolled in the Computer Science Department at the university with varying levels of Cybersecurity experience. The research results did not predominately follow other research patterns. Even though there are multiple, historical instances of one's self-efficacy showing considerable influence on an individual's actions and approach to various threats, results from this study supported the lesser pervasive accounts where it does not. The results were in line with historical instances where self-efficacy did not play an influential part on one's actions. In fact there was no statistically significant difference in the Cybersecurity self-efficacy of freshmen and senior, female and male students. Recommendations for future research include identifying why there was no difference between the groups with a larger research group and post hoc testing.

Keywords: Cybersecurity, self-efficacy, anxiety, deep web, information assurance, information protection, social media, protection motivation theory, technology threat avoidance theory, unhealthy avoidance.

Table of Contents

Dedication

This work and degree are dedicated to David L. Melton Jr. and Sarah B. Melton; my grandparents. Both were giants in their respective talents and faith. Their unwavering devotion to raise me as a man of God and instill within me a love for teaching and educating others runs strong and to my very core. Thank you for believing in me and encouraging me to get this degree. I love you both, and Grandma, I promise I will never forget! Thank you God for your many blessings and not forgetting me.

Acknowledgements

I believe firmly that one person is greater with the support of many as wisdom flows down from one to another. As the culmination of this educational work rests with a degree designation, it could have never been achieved without the support of many others.

Mr. Mike Zeigler is a dear friend, brother, and confidant. He is iron to sharpen my iron and has offered support, encouragement, and spiritual guidance since my academic application to the Doctoral Program at Liberty University was first submitted. His unwavering love and support has guided me through my most difficult times and enabled me to complete this degree.

Dr. Gary Metts has been my dear friend and mentor. Our meeting seemed to be by chance but I firmly believe that God placed this wonderful man in my life. He has guided me through the Doctoral process with expertise and precision. Dr. Metts has been a friend to me when I had few and continually checked on me at all the right times. Without his continual support, I could have never completed this task. He is a shining example of a Christian man, friend, and brother. I will always look up to him and follow his lead.

Dr. Alan Wimberley is the epitome of encouragement. All throughout this Doctoral process, he has continually checked on me to ensure I was progressing appropriately and encouraged me to continue on at all times. His prayers for me were needed and felt. Dr. Wimberley's thought process and reckoning is like no other. He is truly an educational architect and has taught me to think critically and deeply when it comes to educating others. I will take what he has instilled in me and pay it forward the rest of my life.

Dr. Darren Wu has been an incredible inspiration to me. As a member of my educational committee, he has continually and faithfully evaluated the content of my work for depth and accuracy. His thoughts and evaluations of that work make me want to strive harder and seek the

truth in all areas of research. Thank you Dr. Wu for your thought provoking guidance and shining example of what a researcher should be.

Mrs. Caroline Dorinda Melton Helms, my mother. You have always encouraged me during this process and kept Grandma's spirit alive. She is alive in you. Thank you for believing in me and always being there for me no matter what. Your creativity inspires me and while I am not the beautiful artist you are, I take your educational creativeness with me to the classroom. I love you.

CAPT. David M. Melton, my son. You have achieved so many great accomplishments in life. You have taken a lifetime of education from me and used it to serve your country and men and women well in the United States Air Force. Thank you for your continued encouragement and believing that I could do this. I hope to always be a righteous example for you. I love you.

List of Tables

List of Figures

List of Abbreviations

AITP.....Association of Information Technology Professionals

CA.....Coping Appraisals

CERT .....Computer Emergency Response Team

CIA .....Confidentiality, Integrity, and Availability

CPU .....Central Processing Unit

DDoS.....Distributed Denial of Service

DV .....Dependent Variable

IoT .....Internet of Things

IRB .....Institutional Review Board

IV .....Independent Variable

NCCDC .....National Collegiate of Cyber Defense Competition

PII .....Personally Identifiable Information

PMT .....Protection Motivation Theory

SN .....Social Networking

STEM .....Science Technology Engineering and Math

TA .....Threat Appraisals

TTAT .....Technology Threat Avoidance Theory

USP .....Unified Security Practices

CHAPTER ONE: INTRODUCTION

Background

The Cyber World is no longer confined to one's imagination, the covers of a book, or the screen of a movie theatre. It is real and few people are immune to its influence or effects. Regardless of an individual's technological preference or engagement, the world of cyber influences can undoubtedly reach out and alter the course of one's existence. As members of society become increasingly dependent on their smart phones and the use of social media, the simplest acts of functionality or personal interaction can make one susceptible to unauthorized access, fraud, and, liability. As devices become smarter and connectivity is incorporated into the Internet of Things, many homes and businesses are open to monitoring and scrutiny of corporations and nefarious individuals who gain unauthorized access to those systems (Jing, Vasilakos, Wan, & Qiu, 2014).

Historical Context

There are many historical cases documenting individual bullying within an academic environment (Cornell & Limber, 2015). This can happen at any age or grade. In the past, those who were bullied at school escaped the torment once they left the school grounds or entered the safety and security of their neighborhoods or homes. Escape was also found by associating with a different set of friends who had no association with those conducting the bullying. Today, social media has connected the various neighborhoods and friend groups, thus creating an environment for cyber bullying. There are no hours where people can escape the influence of others. The twenty-four hour social media cycle is always active and can have an influence or bearing on one's social standing. This exposure is also magnified as friend networks extend to other friend networks thereby exacerbating the situation. With a few simple misspoken words, a

person's reputation can be ruined. Cyber bullying victims are 2.5 times more likely to do drugs and three times more likely to commit suicide (Davison, & Stein, 2014). The outcome of cyber bullying can be treacherous for anyone including adults and children.

The influence of the cyber world extends beyond normal social networking. It has made its way into the world of academia. As more and more people are working towards higher-level degrees, the need to publish research also increases. While there are many scholarly journals in the cyber world, they can be inundated with publication requests leaving a deficit of opportunity for publication. Unscrupulous individuals are now hijacking journals. Journal hijacking is the process of stealing old or defunct scholarly journal Internet domains or creating a fake journal similar to an actual one (Dadkhah, 2015). As individuals are submitting their research for publication consideration, extreme fraud is taking place. Not only is their research being stolen and sold, so is their personal identifiable information (Dadkhah, 2015). Once the author's information and interest have been made public, they become unwitting targets of phishing and other scams in an effort to steal their monetary resources (Dadkhah, 2015).

The nefarious effects of the cyber world also extend to every day operations such as banking, grocery shopping, and general Internet surfing. This can be done with malware. Malware is malicious software designed to gain unauthorized access to one's information system for nefarious purposes often changing its own software code in an effort to evade detection by signature scanners (O'Kane, Sezer, & McLaughlin, 2011). It can affect laptops as well as smartphones and the Internet of Things type devices. Users no longer have to download an executable file to become infected: information systems compromise can occur when a user clicks on a link or visits a web site. The newest Malware is designed to work across multiple platforms and operating systems posing as valid advertising software (Mattos, 2013). So just by

using common social media applications, users can fall prey to this deceptive software and become susceptible to a compromised information system. Even worse, users can provide pertinent details concerning their personal identifiable information or spending habits. Simple activities such as surfing the Internet can leave users vulnerable and at the mercy of others who intend to inflict harm.

Gaining unauthorized access and inflicting harm is not limited to hackers and criminals. The cyber world's rich environment for anonymity provides the perfect opportunity for groups, organizations, and countries with varying ideologies to make their mark in it. Anonymity is also aided with the use of The Dark Web and Crypto Currency (Smith, & Kumar, 2018). While malicious programs have been used in the past to attack users, now sophisticated software has been developed to specifically attack information systems, in order to gain data and conduct espionage such as Stuxnet and Gauss (Buller, 2013). Advanced cyber weapons are being created and designed to attack both people using various applications, and information system infrastructures containing valuable data (Knopová, M., & Knopová, E., 2014). The aforementioned groups, organizations, and countries, otherwise known as "hacktivists", are attacking others based on ideology in an effort to advance their beliefs or obtain revenge (Herzog, 2011). The cyber world has truly become an active, confrontational environment.

The cyber world exists and hosts an environment of fun, commerce, communications and warfare. Society is unmistakably intertwined and dependent on it. Individuals, businesses, and governments are reliant on the cyber world to operate and carry out their missions. Due to the nature of this potentially hazardous environment, there is an extreme need for qualified information technology security professionals to secure it so that others can safely operate within its confines. It is vital that women and men be skillfully trained in Cybersecurity. As industry

grows, so does the need for highly skilled security professionals. To meet this demand, both commercial and academic institutions are now offering training programs to prepare these people for the challenges faced today. Security certifications and academic degrees are now being offered to those willing to learn the skill.

Societal Context

Historically, the cyber world and Cybersecurity has not been an interest or concern for everyday users. This viewpoint has changed. Unfortunately, individual hackers, ideological based hacking groups, and rogue governments have made it a primary concern for anyone associated with an information system. To defend against the onslaught of attacks, Cybersecurity practitioners must be trained and deployed. Modern companies have vast quantities of intellectual property that represent large amounts of research and development dollars. Years of research along with trials and development have been devoted to achieve this intellectual property. Due to its value, these companies, along with the information systems that store the data, are the targets of attack by foreign governments, competitors, and employees (Fitzpatrick & Dilullo, 2015).

Gaining intellectual property is not the only objective of adversaries. Simply hacking into a network and hitting the "mother lode" is not always realistic. Often hackers must spend hours, days, or months monitoring a network or employee activities to gain a small amount of information that could prove useful in putting together the "big picture". Minor activities such as reviewing the source code of a company's web page or even its product list, customer base, or employee lists can be detrimental (Bressler & Bressler, 2015).

Retrieving information is not limited to reviewing web sites. There is a virtual cornucopia of information listed within annals of social media. Society as a whole is

electronically connected to one another. Participants in this phenomenon often post their activities from going out to eat to where they go on vacation and reveal just how they feel about a particular subject or political matter. Friends who have not seen each other in years are in a position to instantly catch up by visiting a social media page or reading a blog. Individual privacy is minimal at best and that brings to light unique vulnerabilities to one's privacy and personal life. People who were previously living life in ambiguity are now in the spotlight, scrutinized, and often targeted for attack.

Digital natives are people who have grow up with technology ever present in their lives (Christensen, 2016). Without the proper training and implementation of appropriate security practices, many of them fall victim to the unscrupulous activities of others. This often happens when online behaviors are not adapted to match the professional activities of users. This has been seen in medical students who continue to post unprofessional photos, personal identifiable information, and leave social media accounts open for anyone to see (Kang, Djafari Marbini, Patel, Fawcett, & Leaver, 2015). When holding highly visible, professional employment positions, it is crucial that one guards their behaviors and secures their social media outlets to help ensure they are not targets of aggression or the victims of compromise.

Theoretical Framework

There is no mistaking that being plugged into the cyber world brings dangers and risks that must be addressed. They must be addressed with enthusiasm and a well thought out plan of defense. Part of this defense includes having highly trained Cybersecurity professionals. There are also many considerations that must be factored in when considering the qualifications of these professionals. The following questions must be asked:

1. Do they have a certification in a specialty area or in the broad spectrum of security?

2. Do they have a college degree or certificate in Cybersecurity or closely related field?
3. Do they have experience? If so, is it hands on experience in the classroom or in a real life environment?
4. What is their confidence level to effectively meet the Cybersecurity challenges that lie ahead?

The confidence level or the belief in one's ability is a crucial component in this equation. Once evaluated, it can be a determining factor as to how a Cybersecurity professional will approach technological threats and implement mitigation to those threats. These actions are based on the Protection Motivation Theory (PMT), established by Dr. R.W. Rodgers in 1975. The PMT was developed to explain why individuals identify and implement protection mechanisms for human health issues (MacDonell, Chen, Yan, Li, Gong, Sun, & Stanton, 2013). As an example, if a person were to walk out in the middle of heavy traffic, the likelihood they would be struck by a motor vehicle would increase. To reduce that likelihood, they would not walk out in traffic. Likewise, if one were to eat large amounts of salt, their blood pressure may increase. To reduce this likelihood, salt ingestion should be decreased. In both cases, the individual took proper measures to stay safe and protected. This same principle is true in the protection of various information systems within the Cybersecurity environment.

Security threats, whether physical or technologically based continue to happen and it is only reasonable to focus one's resources towards mitigating them. The PMT is partially based on threat appraisals of how serious a threat situation is and then determining how to cope with that situation (Rodgers, 1983). Taking this into consideration, the self-efficacy of Cybersecurity students should be examined. Its primary focus has been on self-health preservation but can be adapted to protect one's health or well being through proper technology protection mechanisms.

Additionally, this can be applied to life and success in the cyber world, electronic commerce, and various social interactions. An example of this would be the compromise of a private bank account or having one's identity stolen. In the event of both situations, an individual could be more susceptible to unnecessary stress that could lead to poor health issues.

The Technology Threat Avoidance Theory (TTAT) is similar to the PMT; however, it focuses specific on perceived technological threats. If a computer user determines that a technological threat is present, they can avoid that threat by implementing the proper security measures to address the issues (Laing & Xue, 2009). The TTAT is a process-oriented view that can assist the security professional as they go through a cognitive thought process in order to arrive at a solution that mitigates the initial threat (Laing & Xue, 2009).

Utilizing principles from the PMT and the TTAT it is possible to understand one's motivation in response to danger as well as their ability to meet it head on and address the situation appropriately. Understanding this motivation and one's ability is crucial in the war against unauthorized access or compromise of an information system directly relating to an individual, corporation, group, or government. In order to properly understand these issues, one could examine the self-efficacy of both freshmen and senior, female and male, Cybersecurity students, as it is the primary foundation of motivation and ability. Self-efficacy is the belief in one's ability to address a particular situation. It has been shown that perceived self-efficacy and personal goals enhance motivation and one's performance (Bandura & Locke, 2003). Bandura and Locke (2003) also show that doubt in one's performance ability provides incentive to learn the necessary skills to meet a particular challenge.

In the case of Cybersecurity, a college age student's self-efficacy is most important, as it constitutes a primary foundation for their future perceptions, interests, and capabilities. Through

standard reasoning, one could surmise that the self-efficacy of a senior Cybersecurity student would be greater that that in the freshman student due to extensive training and life/work experience. Likewise, the motivation of a freshman Cybersecurity student should be high due to their lack of training thus motivating them to want to learn more about protecting information systems against cyber threats. Multiple measurement studies can be conducted from this evaluation such as successful student progression through the program of Cybersecurity study or curriculum quality.

Determining the self-efficacy of Cybersecurity students is vital in order to improve their educational process and prepare them for the work environment. Currently, little research addresses this issue. By conducting this research, great inroads can be made to understand the feelings, motivations, and capabilities of Cybersecurity students and address them appropriately.

Problem Statement

This study addresses the problem of a lack of research pertaining to the self-efficacy of freshmen and senior, female and male Cybersecurity students. While this topic is particularly focused on two small groups of students, there is still little to no research on the self-efficacy of Cybersecurity students as a whole. There is research pertaining to teacher self-efficacy when teaching students how to safely use the Internet, which offers minor insight on Cybersecurity student self-efficacy in principle only. The study developed a scale that measures the self-efficacy of educators, teaching the various information security methodologies and is possibly adaptive to other scientific areas of study that determine teacher self-efficacy (Cavus & Ercag, 2016).

There is an incredible amount of research literature pertaining to Cybersecurity and the cyber world. Topics include cyber bullying, espionage, hacking, and information system

security. Cyber threats are increasing and not only effect individuals but are also a threat to national security (Shafqat & Masood, 2016). There is indeed a need for Cybersecurity professionals that can mitigate security threats successfully. This type of information and research is offered in abundance, but only provides foundational evidence for the need of Cybersecurity experts to address this continuous and ongoing threat.

There is also a large amount of research and information on self-efficacy. A search has also revealed some research on the effects of Cybersecurity training. Some of this research is of particular interest as it focuses on the human relationship in correlation to Cybersecurity threats. Research by Abawajy (2014) has chosen to focus on delivery methods preferences for cyber threat training amongst trainees, as it is a crucial component in addressing the threat problem. It is similar to this research in that it focuses on the human element of Cybersecurity.

The problem is the lack of research pertaining to the self-efficacy of freshmen and senior, female and male Cybersecurity students. Saxena, Kotiyal, and Goudar (2012) stress the importance of student awareness of cyber threats. This in turn can increase self-efficacy, but in no way measures it for freshmen and senior, female and male Cybersecurity students. While there is ample research for student learning and Cybersecurity as a whole, there is little research for their self-efficacy within a Cybersecurity program. Crossler and Bélanger (2014) have moved closer by modifying the Protection Motivation Theory to examine the behaviors of individuals base on perceived threats. Similarly to the Crossler and Bélanger (2014) study and a limited number of others, this research seeks to fill the gap in research and examine the self-efficacy of freshmen and senior, female and male Cybersecurity students specifically. By doing this, it is possible to have a better understanding of student's understanding and internal preparedness toward Cybersecurity threats.

Purpose Statement

The purpose of this study is to determine if there is a difference in the self-efficacy of freshmen and senior, female and male Cybersecurity students. The dependent variable for this study is the self-efficacy of the students while the independent variables are the freshmen and senior, female and male Cybersecurity students. The dependent variable will be measured by a survey created by Phelps (2005) to determine self-efficacy in students. The independent variables, the students, will be equally distributed as either freshmen and senior, female and male Cybersecurity students. They will consist of both freshmen and senior, females and males of any age per grade level. Ethnicity and grade point average will not be a consideration.

The gap in research will be addressed by measuring the self-efficacy of the students and then compared. By examining the self-efficacy of the students, a foundation can be made in order to determine if the Cybersecurity program was effective in preparing students between their freshmen and senior year and addressing gaps between females and males. It will also provide a foundation for future studies to determine if students felt confident and adequately trained to meet the Cybersecurity challenges in a technological environment. By applying principles from the Protection Motivation Theory and the Technological Threat Avoidance theory to Cybersecurity students, it will be possible to determine their security priorities as well.

Significance of the Study

Cybersecurity threats are increasing at an incredible rate. In the past, cyber criminals were primarily responsible for committing all of the cyber crime; that is no longer true. Nation states are responsible for committing a large portion of the attacks against individuals, corporations, and countries (Khan, 2011). Simply, cyber attacks are coming from all directions and can no longer be expected to originate from one group of criminals.

There is also a lack of consensus amongst organizational players as to threat probability and security policy development. In many cases organizations argue over definitions such as Cybersecurity and cyber warfare (Betz & Stevens, 2013). As a result of this discourse, there are varying perceptions to cyber threats, which dictate what level of intensity and methodology will be used to mitigate that threat. One party may see a threat as needing to be address immediately with a vast amount of resources. Another party may have less knowledge of that threat and will not have the background knowledge to address it properly. The second party may not know, what they do not know and are at risk.

This pattern or circumstances can also be present within Cybersecurity students. Young students who are new to a Cybersecurity academic program may know little to nothing about the cyber threats that exist and have little security self-efficacy to address them. Seniors that have been in the program for years and are well trained may have a high level of security self-efficacy toward security threats. When viewed from another perspective, young students may have a high security self-efficacy due to their inexperience and have mistaken perceived ability to handle the threats. Senior students could have low security self-efficacy, because they know how dangerous cyber threats are and perceive the challenge to be daunting.

Research is abundant for self-efficacy and Cybersecurity; however, there is little that is focused on the self-efficacy of Cybersecurity students. By filling this gap, it will be possible to determine how students perceive their capabilities to address Cybersecurity. Identifying this state will provide a foundation to develop academic Cybersecurity programs and teaching methodologies to better address and adequately mitigate threats.

Research Questions

This study seeks to determine if there is a difference in the security self-efficacy of college freshmen and seniors, female and male Cybersecurity students. The sample size is 33 students and the statistical analysis is a one-way ANOVA.

RQ1: Is there a statistically significant difference in the security self-efficacy of college freshmen and seniors Cybersecurity students?

RQ2: Is there a statistically significant difference in the security self-efficacy of female and male college Cybersecurity students?

Definitions

1. *Hacktivists* – Hacktivists are users who attack others based on ideology in an effort to advance their beliefs or obtain revenge (Herzog, 2011).
2. *Journal Hijacking* - Journal hijacking is the process of stealing old or defunct scholarly journal domains or creating a fake journal similar to an actual one (Dadkhah, 2015).
3. *Malware* - Malware is malicious software designed to gain unauthorized access to one's information system for nefarious purposes often changing its own software code in an effort to evade detection by signature scanners (O'Kane, Sezer, & McLaughlin, 2011).
4. *Protection Motivation Theory* – Is a theory developed by Dr. R.W. Rodgers in 1975. Its purpose is to explain why individuals identify and implement protection mechanisms for human health issues (MacDonell, Chen, Yan, Li, Gong, Sun, & Stanton, 2013).
5. *Self-efficacy* - Self-efficacy is the belief in one's ability to address a particular situation. It has been shown that perceived self-efficacy and personal goals enhance motivation and one's performance (Bandura & Locke, 2003).
6. *Technology Threat Avoidance Theory* - The Technology Threat Avoidance Theory (TTAT) is similar to the PMT; however, it focuses specific on perceived technological threats. If a computer user determines that a technological threat is present, they can avoid that threat by implementing the proper security measures to address the issues (Laing & Xue, 2009).

CHAPTER TWO: LITERATURE REVIEW

Introduction

This chapter provides a literature review and theoretical framework that determines if there is difference in the self-efficacy of college freshmen and seniors, female and male students within a Cybersecurity program at their respective university. Cybersecurity self-efficacy can be referred to as an anxiety response to a certain scenario or situation. A sense of security anxiety is defined by how students feel toward protecting or securing various information systems such as computer networks, smart phones, home computers, tablets and other technological devices against unauthorized access or compromise. This incredible paradigm is made even more complex and dangerous with the expanded incorporation of The Internet of Things into everyday lives and activities. As society adds more technological capability and increases access to personal privacy information, do people have quantified anxiety concerning their online safety and security? Are they aware of the inherit risks and threats associated with using interconnected information systems and do they feel the need to protect them? This study will seek to determine if this anxiety exist amongst freshman and senior, female and male Cybersecurity students. It will look at what influences this anxiety as well as the ultimate effect it has on the student.

Comparison

As freshman students enter Cybersecurity programs at colleges and universities, do they have a sense of security anxiety comparative to that of their senior counter parts? Are they mentally aware of the dangers associate with on an online presence? If they are aware of these dangers, do they feel prepared to effectively deal with security threats to the cyber world? Do seniors have an increased sense of security anxiety comparative to their freshman counter parts?

The seniors typically have had years of Cybersecurity training their freshman counterparts have not had access to. Are they better equipped to enter the workforce with a full understanding of the technological risks facing all information systems? Many students are quite adept to using technology but do they have the proper training to guard against security threats? If so, does this training change the security anxiety of the student? Does this ultimately result in a difference between the four groups of students?

Defining Cybersecurity

According to Saxena, Kotiyal, and Goudar (2012) Cybersecurity is the process of protecting personal information and technology resources from unauthorized access gained via technological means. Protecting against known threats is paramount while immediately taking action to mitigate on perceived threats. People implement mitigation procedures for perceived threats based on the amount of risk they are willing to accept (Workman, Bommer, & Straub, 2008). If a perceived threat were high, it would stand to reason that one's anxiety would be high when it comes to mitigating a threat.

Information security also includes protection of data's confidentiality, integrity, and availability (CIA). Confidentiality means that one can be confident that data sent, stored, or received via electronic means can only be seen by those in which it was intended. Integrity is such, that the original format of the data has not been altered. Finally, availability of the data means it is always available when needed (Tamrin, Norman, & Hamid, 2017). In order to protect data and maintain its CIA, rigorous protection mechanisms must be put into place and maintained on a consistent basis. This requires highly trained Cybersecurity professionals who know how to implement this process. They must not only be technically adept but also know the science of business and security. Cybersecurity professionals must be trained in a multitude of

disciplines that range from physical to technical security methodologies. According to Einstein (n.d.), problems could only be solved if one's level of awareness was higher than when the problem was originally created. When this principle is applied to Cybersecurity self-efficacy, students must be aware of the potential dangers that face operations in the information age and must have a certain level of confidence that mitigation procedures to eliminate or reduce technological threats will be effective.

While industry's awareness of Cybersecurity and threats are increasing, the individual, human factor cannot be ignored. Examining one's ability to address and manage the cyber threat must be incorporated into the overall threat assessment. In the field of Cybersecurity, it is widely known that humans are the weak link or a large vulnerability for enabling adversarial unauthorized access to networks and information systems (Anwar, He, Ash, Yuan, Li, & Xu, 2017; Sasse, & Flechais, 2005). When investigating many data breeches, it has been shown that employees are the single point of failure and where many of the breeches are initiated (Thompson, 2016). In order to partially address this problem, one must first look at an individual's self-efficacy as it pertains to Cybersecurity. There are many factors that can contribute to this such as training, past experience, and the technological advancement state of the current threat. If an individual's Cybersecurity training is poor or non-existent, are they adequately equipped to address the threat? In the event that an individual has not had formal training, is their past experience enough to mitigate a Cybersecurity attack? As Cybersecurity continually evolves, is its current state too advanced to be thwarted by an unsophisticated computer student or general user? These factors directly relate to self-efficacy. A highly trained individual may indeed have a high self-efficacy due to that training and thus utilize advanced security methods to mitigate threats. They may indeed feel confident to handle cyber threats

under those circumstances. The opposite can also be true. Individuals with little to no training or Cybersecurity experience may have little to no self-efficacy to appropriately handle cyber threats. There can be an extreme vulnerability when individuals have a high self-efficacy and have no formal training. The self-efficacy differentiation is not limited to users with or without formal training. There can also be differences in genders as well.

When comparing gender differences, it becomes obvious there is a significant gap in various career fields. While females are doing as well as men in math related studies, they are not seeking careers in math at the same rate their male counter parts are (Cheryan, 2012). This can result in a disproportionate number of women in the workforce. Likewise, there are similar differences in the Cybersecurity self-efficacy of women. According to Anwar, He, Ash, Yuan, Li and Xu, (2017) women continually score lower in computer self-efficacy than men. Even though there is a difference in the computer self-efficacy of women from their male counter parts, there is a solution. Amo (2016), conducted a study that also identified a stark difference in Cybersecurity self-efficacy of young girls comparative to that of young boys. This problem was easily corrected with specific training during a weeklong camp that focused on exposing the young girls to Cyber training. By the end of the week, their Cyber self-efficacy was on par and equal to that of the male camp participants (Amo, 2016). This study shows that with the appropriate training, one's Cyber self-efficacy can increase. This also gives credence to the necessity of studying the self-efficacy of female and male Cybersecurity students. This will allow for curriculum evaluation, correction, and implementation based on the results.

Student Anxiety Towards Cybersecurity

There is a plethora of information and research pertaining to cyber bullying, information system security, social engineering, and human intelligence gathering. There has been little

research however, on the comparative security anxiety of college freshmen and senior, female and male students who are studying to become security professionals. In a world where personal information and activities are being continually shared, the paradigm of privacy has changed from decades ago. Social media outlets such as Facebook, Twitter, Pinterest, and Instagram provide convenient conduits for people of all nationalities, interest, and ages to share their personal information and activities with those who are interested thus reducing personal privacy. They also produce an environment for those who wish to gather personally identifiable information (PII) and use it in an unauthorized manner for ill-gotten gain. Unlike other generations, those who are born into this environment are said to be more open and apt to sharing their personal information than their predecessors (Tolmie, & Crabtree, 2018). With that openness, is there a sense of security anxiety in college freshmen and seniors, female and male Cybersecurity students when it comes to protecting their personal information? How do freshmen Cybersecurity students compare to their senior counterparts who have a more training in the field? How do females compare to males within the major of study?

Saxena, Kotiyal, and Goudar (2012), state that industry has been playing catch-up with hackers for years therefore creating a need for Cybersecurity curriculum that produces highly qualified workers in this field. Hackers and those who commit Cybercrime have a distinct advantage over those who protect it. In order to gain authorized access to data or an information system in general, they must compromise or take advantage of at least one vulnerability. Once this vulnerability has been exploited, the chances are high they can successfully achieve whatever goal they want. Conversely, Cybersecurity professionals must have the knowledge, skills, and abilities to identify and secure the many thousands of system vulnerabilities associated with a particular device or operating system. This gives those who wish to commit nefarious

acts a distinct advantage over the Cybersecurity technician. This is why Cybersecurity training is incredibly important. Placing students within a Cybersecurity curriculum is vital and understanding their security anxiety is necessary.

When determining the importance of Cybersecurity student's security anxiety, one must look at both the conceptual and procedural ability of the students. This is accomplished by breaking down one's view on understanding the issue at hand and how to mitigate a threat as well as having the actual ability to carry out the mitigation procedures. A study by Arachchilage and Love (2014) examined whether conceptual or procedural knowledge had a positive effect on a computer user's self-efficacy to thwart phishing threats. It was determined that both conceptual and procedural interaction and knowledge had a positive effect on the computer user's self-efficacy thus resulting in a greater ability to thwart an attack. Having a conceptual knowledge of the immediate vulnerability and threat coupled with the ability to protect against it directly influenced the user's self-efficacy. This increase in self-efficacy enabled users to address the security issues at hand thereby reducing the chance of system compromise.

Understanding self-efficacy within the classroom setting is most important. In the case of a Cybersecurity student with a low self-efficacy it would be necessary to enable that student with the appropriate skills to meet the threat directly. In the event that a freshman student has a high self-efficacy, they might not be fully aware of the potential dangers. Should this be this case, curriculum can be adjusted to make the student aware of the wide breadth of vulnerabilities associated with the field of study in lieu of a limited and concentrated focus. Determining the self-efficacy of freshman and senior, female and male Cybersecurity students can assist in evaluating the success of a curriculum. In the event their self-efficacy is high and coupled with

high grades, one can assume a student knows the imminent Cybersecurity threat at hand and has the ability to mitigate it as needed.

Increasing the self-efficacy of a Cybersecurity student could have beneficial effects. When a student has a high self-efficacy, studies have shown there is a positive relationship between learning performance and engagement (Chen, 2017). Chen (2017) also shows that engagement leads to better performance. When students are engaged and involved in a program of study, they will do better. A with low self-efficacy could lack the interest or dedication necessary to be successful in such a program. Should that be the case, curriculum could then be altered to actively engage the student and increase their interest and thus their self-efficacy.

Theoretical Framework

The Theoretical Framework for the study is based on various progressive factors that contribute to the effective and safe use of information systems and the cyber world. One of the most important factors is to understand the pace of technological growth. Another factor is to identify dangerous technology and quantify the risks associated with using it. Thirdly, one must absolutely have the capability and understand how to mitigate threats associated with all identified vulnerabilities. Once these have been identified, it is crucial to understand one's comparative Cybersecurity anxiety based on technical security training or the lack of it amongst Cybersecurity students. This comparison must also be applied to gender within the same Cybersecurity training environment. To assist in this effort, one must examine the basic principles pertaining on how people protect themselves in various Cyber world situations. There are a variety of self-protection principles that can be directly related to the field of Cybersecurity which also contribute to an individual's self-efficacy. These include but are not limited to the Protection Motivation Theory, the Technology Threat Avoidance Theory, and Unhealthy

Avoidance. By understanding these self-protection principles and mechanisms, one can have a greater understanding of the comparative analysis of self-efficacy amongst freshman and senior, female and male Cybersecurity students.

Rapid Technology Development

Technological advances occur on a daily basis. This can be attributed to the use of processors, also knows as Central Processing Units (CPU). In order to perform the computational tasks, for which a device was created, CPUs must perform millions of calculations per second. Each CPU contains a prescribed number of transistors in which to process the data at a certain speed. Moore's Law (n.d.) states that the number of transistors on an affordable CPU will double approximately every two years. Computer technicians however, state that processing capability doubles each year (Moore, n.d.). This rapid growth and capability has produced an environment in which technology reaches most every aspect of daily life. From smartphones to Internet capable household appliances, to one's front door bell, technology can be accessed from most all walks of life or location. Many industries have become dependent on technology and can no longer function or carry out its mission without it. In some cases, complete economic upheaval can take place with the implementation or deletion of a specific technology (Surry & Baker, 2016). This creates a prime opportunity for hackers and technological manipulators to gain unauthorized access to these devices and information systems that can have a detrimental effect when compromised. In the event of unauthorized access to an information system or PII theft, daily life can be brought to a halt and cease to function. As a result of this work stoppage, there is a need to create an industry that provides protection of these systems.

Many colleges and universities are now offering courses and complete programs pertaining to Cybersecurity. They provide an opportunity for collaborative on-line environments

as well as virtual labs for students to get real, hands on experience (Calhoun, 2017). These programs provide students with the opportunity to learn about the dangers of interconnected networked information systems and how to protect them. As students complete these programs, does their security anxiety increase or reduce? How does it compare with the security anxiety of the freshman students who have not had the same training as the senior students? This anxiety comparison can also be examined amongst female and male Cybersecurity students. To make these determinations, it is essential to study the security self-efficacy of the various groups. It is also necessary to understand the basic principles of self-efficacy and how it relates to the protection of one's self.

Dangerous Technology

The Internet of Things

The Internet of Things (IoT) has quickly become a part of our everyday lives. It is made up of sensors, cellular phones, voice-controlled devices, and computer networks that connect with one another in order to make life's communication seamless and easy. These devices are often hands free and usually accept a compatible device's request for connectivity. Most everywhere one goes, there is some type of sensor that recognizes an electronic device in the possession of an individual. Through these connections, people are able to hail a ride, order desired products, or listen to their favorite songs. They help make every day life easier and more convenient (Atzori, Iera, & Morabito, 2010).

Connection points, wireless access points, and sensors are located in coffee shops, restaurants, and automobiles. No matter where one goes, there is most always an opportunity to connect to the Internet and other devices. Computing and communicating devices located in many different places for end user utilization is commonly referred to as ubiquitous computing

(Weiser, 1993). Simply put, the end user or consumer can always have access to some form of electronic communications. This however, can result in inefficient data transfer and overcrowding. More secure ways of communicating are needed to be developed.

The pervasiveness of ubiquitous computing allows for the collection of many types of data and processing to take place. Sensors located throughout the world and the Internet allow for the collection of many types of data. This makes processing more difficult. The solution to this problem is to incorporate context-aware computing. This is when the sensors are strategically aware of their environment and can adapt to it in order to efficiently process requests from end users (Perera, Zaslavsk, Christen, & Georgakopoulos, 2014). Some view this also as an extension of Wireless sensor networks (Mohsen & Jha, 2016). Most computing devices or information systems have a wireless connection mechanism therefore making this compatible with the current paradigm of data transfer and communications. By incorporating context-aware computing, devices can be devoted to specific tasking therefore making data transfer more efficient. Machine to machine communications are made much easier (Perera, Zaslavsk, Christen, & Georgakopoulos, 2014). This context-aware has inadvertently created a target for hackers to identify specific systems. Knowing what systems work towards a specific end goal can enable a hacker or adversary to gain information ranging from personally identifiable information, banking, or health care. As these communications are made more available, does this ease of use contribute to the anxiety of the Cybersecurity student user?

The Internet of Things was created to make life easier by connecting people and devices to the Internet and to each other. By doing this, data can be exchanged as well as services rendered. Additionally, these devices learn and document the preferences of its users. Little to no interaction is needed from an end user when a specific action is taken on behalf of that user

by the devices to complete a desired effect (Dohr, Modre-Opsrian, Drobics, Hayn, & Schreier, 2010; Perera, Zaslavsk, Christen, & Georgakopoulos, 2014). This can include ordering products off the Internet or playing music at a specific time of day. This creates an incredible convenience for the end user that becomes an everyday part of life. Due to its insertion in daily activities, people can become dependent on it therefore making it most difficult to remove it from one's life (Nolin, Olson, Högskolan, & Akademin, 2016). This creates interdependence that can be somewhat difficult to do without. Does this ease of use lower anxiety and increase Cybersecurity self-efficacy?

The IoT interdependence seems to be included in most every aspect of life. There are smart buildings; healthcare monitoring stations, smart vehicles, construction management, assembly line management, and food supply chain management (Mohsen & Jha, 2016). These areas make up some of the most important aspects of human life. While it is good these areas work smooth and efficiently, their operations are deeply rooted in automated data transfer. Does this come with risks? Are there vulnerabilities with such interdependence on technology? Are users aware of potential risks? Are adversaries such as foreign governments, or ideologically based groups targeting these systems for disruption? Most importantly, are the innovators and users of this technology aware of the potential dangers associated with its implementation? Can these factors effect one's Cybersecurity self-efficacy?

There are many modern conveniences provided by IoT but with those conveniences come many vulnerabilities and risks that can cause harm to those who use it. Like all information systems, the IoT is vulnerable to attack. IoT smart devices are unusually susceptible to compromise do their very open architecture and inability to take advantage of the advanced security safeguards that are available due to technological limitations (Radisavljevic-Gajic, Park,

& Chasaki, 2018). Multiple attacks exploiting this weakness abound. One such attack is a Distributed Denial of Service (DDoS). This is where an information system is overwhelmed with data or requests for data beyond that which its processor can handle thus rendering the device in a continuous loop and unable to operate.

A DDoS is particularly effective with the IoT devices for the following reasons (Bertino & Islam, 2017):

- IoT devices are autonomous.
- IoT can control other IoT devices.
- Ill-defined configuration parameters.

The IoT devices have very little, customized administrative capability and are prime candidates for a DDoS attack. Many IoT devices are not being created with a built in security defense system (Bertino, Choo, Georgakopolous, & Nepal, 2016). This creates a prime opportunity for targeting by hackers and adversaries. Other devices that have been compromised can overtake IoT devices that are created without a security mechanism. This creates a vast chain of insecure networks.

The IoT hardware devices are not the only component that is vulnerable. Each device has specific software that enables it to complete its purpose. In some cases this software is written quickly or without proper analysis for security vulnerabilities within it. This software can be compromised which allows the entire systems to be compromised (Abomhara & Koien, 2015). As the numbers of IoT devices continually grow, so will their vulnerabilities. One can rightfully assume that new methods of machine-interaction will be developed. This should include web interface development via smart phones as well as biometric capabilities that include voice and human characteristic recognition. These developments must keep pace with the absolute demand

for increased capability and rich feature sets. Other vulnerabilities include inferior device firmware, insufficient transport encryption, and insecure network services (Tait, 2017).

There are three basic domains in which the IoT works. The first is the sensing domain in which electronic measurements are taken to determine various conditions such as electricity usage. The second is the social domain that congregates multiple users in similar groups with similar interests to exchange information common to all. The third is the mobile domain where users share information on a user-to-user basis (Zhang, Liang, Lu, & Shen, 2014). Associated with each of these domains is an IoT attack called Sybil. The basic premise of this attack is to fraudulently present the credentials of another entity. There are three variants of this attack aimed at the three domains. Each Sybil variant will present itself as a false sensor, a false personal user, or an authorized peer-to-peer device (Zhang, Liang, Lu, & Shen, 2014). With the implementation of these attacks on the various domains within the IoT, an adversary can obtain unauthorized user information to use for a variety of nefarious purposes. As more and more people and industries are becoming dependent on the IoT, the opportunity for information compromise increases as well. Are people prepared for this situation? Moreover, does the general user population of the IoT know of the risks and vulnerabilities? For those who do know of the potential compromise, do they know how to address the situation properly? Does this contribute to or decrease one's anxiety or self-efficacy?

The IoT has created an incredible opportunity for users of electronic information systems to reduce time, increase convenience, and stimulate innovation. It is fun to use and could possibly be the precursor of in-home artificial intelligence. As people use the IoT, they will inevitably find uses for it while engineers will continue to develop its capabilities. It has already found its way deep into commerce and entertainment alike. With its continued use and growth,

adversaries will also continue to identify vulnerabilities and use them to their advantage. Their motivation can be ideologically or personally based, or both. Regardless of the purpose of their attacks, one can absolutely surmise they will continue and grow.

As the IoT and its usage grow, there is also a need to see awareness education grow as well. There are multiple reports of industry data breeches. These breeches take place at both large and small organizations. The attack and data breach of Sony Pictures made international news and was showed that large organizations were still susceptible attack and compromise (Haggard, & Lindsay, 2015). The mass retail chain, Target was also a victim of unauthorized compromise and data theft (Manworren, Letwat, & Daily, 2016). Based on this information, large businesses can fall prey to unauthorized access and data theft. They also affect individuals and their families. Personal identifiable information is stolen, sold, used leaving a wake of destruction in their path. This is evidence that adversaries never give up. An educational campaigned must be convened so these attacks have minimal effects. The average IoT user has no idea of these vulnerabilities. While Internet super users may have heard of these issues, one must ask if they know the specifics of these attacks and how to mitigate them.

The Dark Web

Many people in mainstream society utilize the Internet to conduct business and socialize. Communication forms such as texting and video conferencing offer a personalized and unique way of getting one's message to another. Unfortunately, there are individuals or adversaries on the Internet that choose to use it for nefarious purposes. They take other people's information and data that cross the Internet on a daily basis and use it to gain financially or politically. Personally identifiable information (PII), medical records, and banking transactions are just a few of the information targets that adversaries collet. Many people are unaware of the specific

techniques used to steal their information and can be unprepared to protect it. Entities or nodes on the Internet, in its current form, communicate via Internet Protocol (IP) addresses and Domain names. Various servers, routers, and communication pathways support data transfer between these names and addresses. Regulatory bodies and organizations also monitor these pathways. While they cannot be monitored for all activities, there are standards and protocols that assist the regulators and law enforcement agencies in maintaining law and order. This current Internet architecture operates as a top-level domain. There is an alternate layer beneath the top-level domain servers that operates a sinister environment where illegal activities occur known as the Dark Web.

The Dark Web is a layer of the Internet that supports, terrorism, illegal activities, and the distribution of child pornography (Bradbury, 2014). It is assessable by the use of specialized software that enables the end user to access specific web sites that are intended to be out of site from the general public (Bradbury, 2014). The Dark Web is also a prime environment for the sale of illegal firearms and weapons of destruction (Spalevic & Ilic, 2017). With the use of specialized browsing software such as Tor, individuals or organizations that wish to operate outside the realms of standardized regulation or law can do so with a certain degree of anonymity. They can operate in an environment that offers them virtual anonymity (Spalevic & Ilic, 2017). Activities such as money laundering, hit men for hire, and illegal weapon sales take place on a daily basis (Bradbury, 2014).

The Dark Web is not only used by everyday criminals but terrorists as well. There has been a significant increase in terrorists' activity on the dark web (Weimann, 2016). It is being used to transfer money, facilitate meetings, and conduct research for future attacks and provides an ideal environment for user anonymity (Weimann, 2016). After the terrorists attack in Paris,

the Hacktivists group Anonymous targeted hundreds of ISIS sponsored web sites for destruction. It was then that ISIS went to the Dark Web to spread their message and coordinate future attacks and illegal activities (Weimann, 2016). Knowing these facts, one might ask how all this activity on the Dark Web affects them.

Affects of the Dark Web

There are many illegal activities that are conducted on the Dark Web. These activities support many different groups and agendas. Some are state sponsored in an effort to support a political cause while others are ideologically based and founded on an individual's or group's beliefs. This is often the case with al-Qaida or ISIS. If illegal activity on the Dark Web is ideologically based, how does that affect the every day user of the Internet? The answer is quite simple; money. All organizations whether good or bad, need money to finance their operations. When large organizations are breeched and PII is stolen along with credit card numbers, that information can be sold for cash to fund the adversary's cause. It was recently reported that over 200 million Yahoo user account information had been stolen and sold on the Internet for approximately 3 Bitcoins (Rizzo, 2016). Bitcoins is a type of Crypto-currency created by a person using the alias Satoshi Nakamoto and has no transaction fees or standard worldwide regulation. (What is Bitcoin?, n.d.). It is also most difficult for the Internal Revenue Service (IRS) to track or regulate. Hackers and adversaries also can use other user's identity to establish credit, which can be used to obtain funds as well. The problem does not stop there. These organizations grow stronger each day they can operate outside the bounds of law and regulation. As they grow, so does their mission and impact which ultimately affects law-abiding citizen's lives and safety.

The Dark Web and Social Networking

There can be no doubt that Social Networking (SN) or Social Media (SM) is a societal mainstay. Regardless if one is sharing family pictures, keeping up with loved ones from long distances, or reacquainting themselves with a friend from their early years, SN plays an integral role in a large portion of the population with access to the Internet (Gundecha, Barbier, Tang, & Liu, 2014). As it has grown in recognition and popularity, the Dark Web has provided a social networking haven of sorts for those who want to skirt regulation and conduct themselves on-line in any manner in which they see fit; it is an alternative to upper-level domain social networking (Gehl, 2016). This attraction to the Dark Web creates an incredibly dangerous environment for those unsuspecting users seeking independence and freedom, to fall prey to those people and software that intend to do harm. Utilizing the specialized software needed to access the Dark Web can often come already compromised with computer Trojans and tracking software. As each site is visited on the Dark Web, the users will open themselves up for technological compromise for zero day viruses as well as custom viruses that have not been reviewed or have virus definition files for. The Dark Web is absolutely no place for curious users to explore!

Protection Motivation Theory

With all the inherit dangers associated with the Internet and the connection of various technological systems, it becomes vital that users be aware of these threats and be able to protect against them. Many information systems and technological based devices have built in security mechanisms. This can be hardware or software based. Hardware devices can include physical locks as well as external appliances such as secure routers and firewalls that prohibit the flow of information up range to a vulnerable receiving device. Software security mechanisms range from anti-virus software, screen locks, and specific programs that look for anomalies. There are

a plethora of security mechanisms for use by the end user such as anti-phishing filters and anti-virus software (Lim, Park, & Lee, 2016). As such, it is possible for end users to become reliant on these devices and forgo their personal responsibility to protect ones self. Proper training can offset this response. With the implementation of appropriate training, the rate click for computer induced Phishing scams reduced significantly due to a better informed and prepared user (Lim, Park, & Lee, 2016). The results of the aforementioned study show that training does have a positive effect on the end user's ability to address security threats to information systems. When properly trained, individuals will protect themselves against threats. These actions coincide with the Protection Motivation Theory.

Anxiety for protection of information systems can be mapped to the Protection Motivation Theory (PMT) theoretical framework established by Dr. R.W. Rodgers in 1975 to better explain why individuals identify and implement protection mechanisms for human health issues (MacDonell, Chen, Yan, Li, Gong, Sun, & Stanton, 2013). It is made up of two main principles, Threat and Coping Appraisals. A threat appraisal assesses how serious a situation is while a coping appraisal assesses how the situation will be responded to (Rodgers, 1983). This translates into Cybersecurity in that threats must be identified and mitigation procedures put into place to eliminate that threat.

The PMT can be applied to the Cybersecurity student and their level of anxiety thus effecting how they respond to various threats. In the even that a freshman student has low anxiety it could be attributed to a sever lack of exposure. That student may not have the necessary information to be concerned about Cyber threats and therefore have a low anxiety. The same could be said for a senior student. In the event their anxiety is low, they may feel they are adequately trained and can handle the threat. The reverse can also be stated. Freshmen who

have a high anxiety may have the training or simply be nervous concerning the unknown. Seniors who have high anxiety can fully know how serious a threat is and how difficult it will be to mitigate it. By utilizing the PMT and evaluating each student's motivation, the approach to address their anxiety can be determined.

The Protection Motivation Theory has been used in multiple instances to determine Cybersecurity motivation. When using PMT, threat appraisals in some on-line safety studies were shown to be a predictor to Cybersecurity protection intention, however in other studies, perceived threat capability was shown not be a factor in determining if someone would implement security mechanisms or not (Tsai, Jiang, Alhabash, LaRose, Rifon, & Cotten, 2016).

Technology Threat Avoidance Theory

Technology Threat Avoidance Theory (TTAT) states that if a computer user perceives there is a technological threat, they will avoid the threat by implementing security measures; if the threat cannot be avoided, they will passively avoid the threat through emotional coping mechanisms (Laing & Xue, 2009). This is similar to the Protection Motivation Theory (PMT). By using a process-oriented view, this theory delineates how computer users go through a cognitive thought process and derives a protection mechanisms, however, it does not introduce influential factors that help them to arrive at their decisions (Laing & Xue, 2009). By combining the TTAT and the PMT, not only can threats and mitigation procedures be identified, the influential factors can be identified as well.

These two theories help establish the motivation behind the anxiety of individuals to address a situation. They are based on self-protection and seek out threats while identifying ways to reduce or eliminate the threat. This is directly applicable to the anxiety of Cybersecurity students within the current college environment. By the time students go to college, they have

been using technology most or all of their lives; they are digital natives. Those who have a technology gap, digital immigrants, have had a time in their lives in which technology has not been a major presence. Digital natives do not have the gap (Christensen, 2016). Both digital immigrants and natives have the opportunity to be exposed to technology and will most likely have reasonable amounts of experience with it. In fact, there is no consensus or empirical evidence that shows there is a significant difference in the computer self-efficacy of digital immigrants or digital natives (Teo, 2016).

If there is indeed no general consensus or empirical evidence that shows a significant difference between digital natives and immigrants, then further examination must be undertaken. Cybersecurity programs are offered in many colleges and universities. These programs can be accessed both in the classroom and online thus providing exposure to students of any age. While there is no guarantee that freshmen students will be digital natives, it still provides the opportunity for the evaluation of older students perspectives that could possibly have little to no training in the field of Cybersecurity.

With varying degrees of experience comes exposure to technological threats such as viruses, malware, software Trojans, and unauthorized access. It is possible that both groups could have dealt with security breaches and issues thus forming an opinion concerning the need for Cybersecurity resulting in a discernable and measureable self-efficacy. This will undoubtedly translate into a certain amount of anxiety that will determine their participation in the security process.

Importance of Cybersecurity

Technology impacts many aspects of society. There are multiple industries that must have secure networks to ensure consumer confidence and stable operations. Both the banking

industry as well as the military must have secure communications within their networked information systems. Banks are the victims of ever increasing attacks against their networks. To help ensure consumer confidence, they implement a variety of security methodologies such as firewalls, encryption, intrusion detection and prevention systems, and password protections to name a few (Moin, Zarka, & Karuna, 2016). Amongst its many technically based security safeguards, Moin et al. (2016) state that user awareness programs are necessary to help ensure that the overall environment is kept safe. End users are among the key components that help ensure computer security. They will however, become the weakest link if they are not made aware of the security threats that are in existence and how to deal with them effectively (Arachchilage & Love, 2014).

The United States Military is a world leader in technologically based warfare and is joined by other nations such as China (Warikoo, 2013). Cyber warfare is not just in the movies and a subject of fiction; it is real and is a realm that must be protected. One of the primary targets of the Chinese government is the intellectual property of the United States (Warikoo, 2013). By stealing intellectual property, other countries can reduce the cost of research and development and produce technically advanced weapons at a much cheaper price while reinvesting the saved funds back into the production of the weapons they are producing. Intellectual property makes up the specific build details of a product or process. This is applicable to weapon systems, information systems, space systems, and communications systems. In the event these plans are stolen, the products or systems can be reproduced by reverse engineering and possibly improved on. It is crucial that this information be kept private and in the hands of the rightful owner. In the event this information is lost, the resources used to create them in the first place by the original producer is lost and wasted. Multiple security

mechanisms must be put into place to protect this information along with the staff with specialized technical expertise to implement and effectively maintain the security. Martinez and Kayser (2013) state that threat information must be shared between military entities in an effort to combat threats to information systems. Threat identification and mitigation procedures must be made available to all concerned parties so that awareness is raised and protection mechanisms can be put into place to prevent further loss or system compromise. Cybersecurity must be maintained in order to protect the United States' intellectual property as well as maintain its technological superiority (Warikoo, 2013).

Necessity of Cybersecurity

The field of Cybersecurity is growing at an incredible rate in the United States and world. Most every conceivable public entity has access to the Internet and electronic communications. These entities include businesses, hospitals, schools, civic organizations, local and federal governments, and the military. Cyber crime is growing at an alarming rate and as of 2015, costing businesses between 400 to 500 billion dollars per year (Morgan, 2015). With every new electronic capability or technological advance comes the threat of unauthorized access to information systems and devices. These information systems consist of and are not limited to the Internet in general, smart phones, databases, computers and networks, medical equipment, military assets, communications equipment, satellites, smart industrial equipment, and home appliances. Much of the entire world is online and connected by some means of network communications. Due to these connections, network security is vitally important as computer crime is on the rise and will most likely to continue to grow at an accelerated rate (Wiener-Bronner, 2014). Due to these threats, it is vital to mentor and train Cybersecurity professionals to defend against them. Threats to the cyber world increase all the time. According to Craig,

Shackelford, & Hiller, (2015) 96% of the Cybersecurity firm's 1600 monitored networks were hacked in 2015. Defense is a never-ending battle that has resulted in a concept called Active Cyber Defense. This is where Cybersecurity experts actively seek out potential threats and eliminate them before they can cause problems. This search for potential threats is also accompanied by appropriate policy, legal legislation, and regulatory framework development (Craig, Shackelford, & Hiller, 2015).). This proactive movement also includes the identification and implementation of industry best practices to help eliminate activities that would open the door to potentials hackers and Cyber criminals (Shields, 2015). By implementing best practices, users could help minimize careless activity while helping to ensure the network's security.

Social Media

With the advent of Facebook, Twitter, and other social media outlets, society repeatedly shares its activities with the world. Personal thoughts, activities, and photos are continually posted. Privacy has taken a back seat to that of sharing information. Sharing information seems to have become a favorite pastime thus leaving a prime opportunity for adversarial entities to take advantage of the information overload for their financial or ideological gain. Unfortunately, many people are unaware of the dangers of sharing their information on online community forums. This may contribute to either a low or high Cybersecurity self-efficacy.

Due to the rise in unauthorized access or hacking into various information systems, the need for protecting these systems is of vital importance. There is a need for Cybersecurity professionals with the skills to effectively address the threats at hand. While there are a number of professional security organizations such as SANS and ISC2, that provide training in these areas, there are also many colleges and universities that are creating Cybersecurity programs and majors. These programs of study have been developed to train students interested in

Cybersecurity to defend both private and public network and information systems from hacking, compromise and unauthorized access.

Security Methods

There are several security methods that one would surmise to provide an information system user with a certain amount of personal protection with the implementation of those methods. They include but are not limited to the proper usage of passwords, unhealthy avoidance, proper system configuration, Cybersecurity training, and the overall awareness that threats exist within this realm. Certainly, these protections offer some sort of assurance of Cyber health and well-being. These protections are good but do not negate the failing of the best of intentions or general negligence. Studies show that despite the best implemented security controls, that people themselves are the weak link in security. Personality traits or threat perceptions may have a significant impact on how an individual approaches Cybersecurity (Shropshire, Warkentin, & Sharma, 2015). Even though individuals want to address the Cyber threat, they may be unable to, given their personality traits or even simply overlooking the subject of security all together. These actions have the ability to short circuit the technological security mechanisms and provide an avenue for intruders to enter an unauthorized domain. Should this trait be prevalent, it is possible for one's security self-efficacy to be minimal despite appropriate training. In order to provide a comprehensive analysis of one's security self-efficacy, it is vital that multiple security methods be examined and taken into consideration. Simply reviewing one will not provide an adequate answer on their direct impact on student anxiety level in relation to Cybersecurity self-efficacy.

Password Usage

There are multiple security methodologies that are utilized to help prevent unauthorized access. One of the most widely used practices is to implement passwords. Passwords are a good first line of defense to prevent an adversary from gaining access to technological assets, accounts, and information systems. Various systems require that passwords consist of special characters, upper and lowercase characters, special characters, and specified lengths. At times, this process can be cumbersome and tedious. They are also subject to being entered incorrectly as well as forgotten by the end user. To help avert these issues, users write passwords down, store them on pages of books, and make them easily obtainable by unauthorized individuals. This creates an environment that provides adversaries with the opportunity to gain unauthorized access to a particular system. Even though users create prime opportunities to circumvent mechanisms with little challenge, Knott and Steube (2012) report that 94% of the people they surveyed found that password security was important. A majority of the students surveyed - 57%, however, were interested in obtaining a tool that would automate password management (Knott & Steube, 2012).

Unhealthy Avoidance

Computer security can be thought of as a good practice until the security methodologies and practices become so tight and ridged that functionality ceases to exist. Is there a delicate balance between being aware of computer security practices and actually free and uninhibited functioning to accomplish a task? Can one be so aware and concerned about Cybersecurity to where their anxiety becomes chronic? In the quest to accomplish necessary or perceived necessary activities, it is possible for a technology user to forgo all security practices in the name of getting things done. In this case, all security functionality would be eradicated to make

productivity much easier. When implementing security, an often easily attainable result is to slow down system processing, increase steps to completion, and make the overall task cumbersome. In the event that a task becomes too difficult, one can be easily tempted to ignore threats and security vulnerabilities? Due to this unwanted difficulty could the end user possibly avoid security practices all together?

In a study by Mannarini and Boffo, (2014), it was determined that a middle level of anxiety was associated with the highest levels of security while high levels of anxiety were associated with low levels of security. There are multiple ways to incorporate these findings within the unhealthy avoidance framework. When individuals are feeling a middle level of anxiety associated with a high level of security, are technological assets adequately protected against Cyber threats? Are those individuals solely relying on automated security mechanisms to ensure unauthorized access does not take place? As technological security mechanisms are implemented and security anxiety relaxes will the individual become the weak link in the chain of security? As anxiety rises with lower levels of security, will the end user find the need to incorporate a proper mix of individual and mechanized security features? Due to these anxiety levels, will users simply avoid the stress of it all?

The aforementioned questions are difficult in nature and require further examinations. These issues can be addressed by looking at the self-efficacy of Cybersecurity students. While answers cannot be totally achieved with one study, it will provide a solid foundation for future ones.

Security Training

Freshman to Senior

Freshmen enter college with a certain amount of Cybersecurity training as derived from life experience, high school academic training, specialized clubs, or self-study. They can be trained or share peer to peer experiences via computer clubs such as the Association of Information Technology Professionals (AITP). Science, Technology, Engineering, and Math (STEM) programs can also offer well-developed and organized programs of study in the field of Cybersecurity. Various competitions such as the National Collegiate Cyber Defense Competition (NCCDC) can provide an environment of learning and awareness for them to compete against others in their field and hone their skills. Each of these methods has the ability to raise Cybersecurity awareness in the students. However, do they do enough? Are students taking advantage of the opportunities? In the event that a student does not take part in these programs or does not have the resources to be included, they may enter a collegiate Cybersecurity program with little or no experience. Do colleges surpass these programs or can college bring the inexperienced student up to speed?

As freshmen enter Cybersecurity programs in college, the specific study materials offer little hands on instruction (Meso, Ding, & Xu, 2013). Much of the program is theory based in some cases. This can leave the Cybersecurity student with only a theoretical knowledge of security principles. By having limiting collegiate hands-on experience, students continue through the Cybersecurity program and enter the workforce with only the experience they received in high school, computer clubs, and associations. With this limited experience, are they equipped with the proper and appropriate sense of security anxiety? Do they have the proper skills to address Cybersecurity threats? Chances are, without proper training, students cannot

adequately comprehend the severity of the threats caused by malpractice within daily information technology operations (Meso, Ding, and Xu, 2013).

Cybersecurity Awareness

There is an ever-increasing amount of data exchange amongst systems and people (Kim & Yong, 2012; Mejias & Harvey, 2012; Mejias & Balthazard, 2014). With the large exchange of data, users have several options in which to operate. They can either be aware of the security threats and protect against them or participate in data exchange blindly without any consideration to the possibility of their activities being compromised by unauthorized user access and intervention. Unfortunately, security is not usually the primary concern of users and software or system developers (Pfleeger & Caputo, 2012; Mejias & Balthazard, 2014). At some point during information systems operations, there must be an awareness of information security or Cybersecurity.

Cybersecurity awareness is the knowledge of individuals or systems of the possibility of cyber attacks against those systems and the negative impact they can have on an organization or entity (Kruger & Kearney, 2006; Liang & Xue, 2009; Mejias & Balthazard, 2014; Pfleeger & Caputo, 2012). There are various models in which to measure this awareness. Mejias and Balthazard (2014) state that models and assessments help raise the Cybersecurity awareness of individuals. Unfortunately, not all users have access to these models and assessments and do not reap the benefits of them. The Cybersecurity awareness of the average college freshman can be lacking or must be derived from other means.

Cybersecurity Awareness Training

Due to the increasing use of technologically based devices in people's everyday lives many users may experience some sort of exposure to potential security threats or prevention to

those devices. While their Cybersecurity awareness can be derived from experience, how many of those individuals are exposed to organized security training? A study by Kim (2014) surveyed 67 college students ranging from freshmen to seniors as well as graduate students to determine their level of Cybersecurity awareness. Kim's (2014) study showed that many students did not participate in the formal Cybersecurity training at the university in which they attended and did not have a full comprehension of security practices. Kim (2014) did note however, it was desirable to change the type of training being delivered to correspond to present day threats. This would make the training more pertinent and useful. Life experience can indeed expose students and users of technology to persistent threats, however formalized training is good and can provide benefit. As Kim (2014) pointed out, not all students take part in the training. It should also be noted that not all training is good training. The implementation of conceptual based training and the lack of hands on activity could possibly leave the student ill prepared to handle threats to information technology in a proper fashion. Finally, it is most important to not only have the Cybersecurity training but to encourage and ensure that students actually take the training (Kim, 2014).

Changing Training to Address Student Practices

Student awareness of Cybersecurity can come from life experience or from formalized training. Their level of their awareness however, can also be based on the content of the training and how it is related to events that happen in their lives (Slusky & Partow-Navid, 2012). According to Slusky and Partow-Navid (2012) security awareness training must cater more to the student's practices. If a student is predominantly using social media, security training in the area of telecommunications will have little value. If most students are utilizing their phones as the primary conduit to the information super highway, desktop computing training will not assist

them in operating in a more safe and secure manner during their daily activities. Regular college Cybersecurity curriculum in itself is simply not enough to raise student awareness resulting in best practice (Slusky & Partow-Navid, 2012). The training needs to be content specific as well as include college instructors and administrators to help ensure the overall environment is kept safe (Slusky & Partow-Navid, 2012).

Cybersecurity Training and Social Media

Social media sites such as Facebook, Twitter, Pinterest, and Instagram are easily assessable by anyone with access to the Internet. General observation will undoubtedly reveal many college students on their phone and connected to these sights. Have these students been trained to implement appropriate security measures when using these sites? Are they aware of social engineering and human intelligence gathering techniques used by various individuals groups and countries? Have they been made aware of the extent in which these activities exist? In a study by Mensch and Wilkie (2011) people have been determined to be the Cybersecurity weak link and the end user is ultimately responsible for implementing a certain measure of security.

Social Media in the Classroom

Social Media is currently being used in the classroom. Schnackenberg, Vega, and Simard (2014) state that in response to a high demand with limited seating availability, colleges are incorporating social media activities to accommodate students wanting to take the class. Other technologies also included interactive white boards, cell phones, and computer tablets (Schnackenberg, Vega, & Simard, 2014). Typically, one would deem the use of new technology within the classroom as good. It is not without its drawbacks. All technology has the potential to have vulnerabilities. As students enter the classroom or are on-line using social media, these

vulnerabilities are present whether they are seen or unseen. Are the teachers prepared to address them? Are the students? Has the Information Technology Department of the school assessed whether the vulnerabilities present an acceptable risk and do the students have adequate training to engage in appropriate security behavior while using them? Are the teachers focused on presenting the materials without giving proper consideration to the vulnerabilities that arise when these sites are used? Most importantly, are the students blindly following without knowing the inherit risks they are taking?

The use of technology is ever present in most aspects of life. It is pervasive in most civilized societies. Even the youngest of persons has access to technology. Both businesses and individuals use it to successfully carry out their endeavors. As the inclusion of technology in daily life has produced many benefits, it has likewise produced more than ample opportunity to commit illegal activities. Exposure to these activities can result from using personal computers, email, smart phones, and many other types of electronic communications equipment. Hackers are not only targeting primary information systems but also secondary ones such as automobile computers as well as medical equipment. Due to this type of exposure, are users more security conscious? Has this environment produced a certain amount of security anxiety amongst its users? Do students entering college have any awareness of the threats that are posed from being attached to the Internet?

Focused Summary

What Is Known

In an effort to improve the educational process and student preparedness for the mitigation of advancing Cyber threats, it is vital that the self-efficacy of freshmen and senior, female and male Cybersecurity students be examined. Self-efficacy has been studied for years

and can be described, as the belief in one's self to successfully accomplish a particular task. It has been shown that a high self-efficacy does indeed increase ones ability to meet challenges head on. When combining self-efficacy with Cybersecurity, it is possible to gain insight into a student's security anxiety in relation to their ability to address Cyber threats and mitigate them as necessary.

Self-efficacy produces low levels of anxiety. If a student has a high level of self-efficacy, their anxiety level drops. Mannarini and Boffo, (2014), determined a middle level of anxiety was present with the highest levels of security while low levels of security produced the highest anxiety. Simply, when security mechanisms were put into place, either automated or humanly implemented, individuals had less anxiety. In a study by Bellini, Filho, de Moura Junior, and Pereira (2016) it was shown that high computer self-efficacy and low anxiety did not promote voluntary technology usage while extremely high computer self-efficacy and extremely low anxiety may undermine technology usage. If self-efficacy was too high, technological security was not very well implemented.

What Is Unknown

Very little work has been done in the field of monitoring student self-efficacy within Cybersecurity programs. There is little to no focus on this specific group of people. Due to this lack of research, there is little information on the causation or consequences of Cybersecurity self-efficacy amongst students. Are there differences in the self-efficacy of freshmen and senior Cybersecurity students? Are there differences in the self-efficacy of female and male Cybersecurity students? If there are, what are they and what is the cause?

The Study Addresses Gaps In Literature

This study absolutely addresses gaps in literature by seeking to determine if there is a difference amongst variables, namely freshmen and senior, female and male Cybersecurity students relating to their self-efficacy. Once a determination is made as to the differences, further research will need to be conducted to identify the cause and effect of the positive or negative relationships of the four groups. This basic study serves as a positive foundation and basis for future studies. By conducting this study, steps can be taken to alter curriculum to limit the differences and better the students within the program to face the Cybersecurity challenges that face them in the future.

CHAPTER THREE: METHODOLOGY

This chapter describes the methodology used to determine if there is at difference in the sense of security self-efficacy amongst college freshmen and senior Cybersecurity students. It identifies the research design, questions, participants, settings, instrumentation, and procedures used to gather data, and data analysis to address the null hypothesis. Specifically, this study examines the student's level of self-efficacy toward the Cybersecurity threat and their preparedness to address that threat while effectively implementing mitigation. Self-efficacy is the belief in one's ability to handle or deal with a particular situation (Crossler & Bélanger, 2014). While the use of various types of information systems is pervasive, there are individuals that do not know the types of threats commonly associated with them. They are ill prepared to harden or secure the systems leaving them with feelings of insecurity and uncertainty. On the opposite end of the spectrum, there are users that do know the threats as well as how to defend against them. When dealing with Cybersecurity threats, it is imperative that one knows the vulnerabilities, risks, and their mitigation. If this information is unknown, it can leave the end user with a lack of security self-efficacy or in a state of pure ignorance.

Cybersecurity programs offered at colleges and universities are designed to educate the student to identify, protect, and defend against information systems threats. This defense not only includes professional, working environments but personal use as well; this includes smartphone usage as well. Using basic logic, it stands to reason that freshmen entering a Cybersecurity program at a college or university would have little experience in the identification and mitigation of cyber threats and that seniors would be well prepared after completing a Cybersecurity curriculum. With that preparedness, logic would also dictate a high level of one's security self-efficacy; the ability to deal with cyber threats appropriately. Using

that logic, it stands to reason that freshmen would have a low level of security self-efficacy. Is this indeed the case? Is there a difference between freshmen and senior students Cybersecurity self-efficacy? Additionally, is there a difference between females and males? This study will examine those issues.

Design

The design for this quantitative study will be non-experimental, causal-comparative otherwise known as group comparison and will be used to determine if there is a causal relationship between variables (Gall, 2015). It will be used to determine if there is a difference in the level of security self-efficacy for Cybersecurity students at small, southern university. The students will be in two different groups made up of freshmen and seniors as well as females and males, which make up the independent variables. Their level of security self-efficacy will be the dependent variable. The target of the study is to determine if there is a difference between the students therefore prompting further study to identify the cause of the difference or identify why there is no difference.

Research Questions

The purpose of the study is to determine if there is a difference, in the security self-efficacy of college freshmen and seniors, female and males who are Cybersecurity Students.

RQ1: Is there a statistically significant difference in the security self-efficacy of college freshmen and seniors Cybersecurity students?

RQ2: Is there a statistically significant difference in the security self-efficacy of female and male college Cybersecurity students?

Null Hypotheses

$H_0$1: There is no statistically significant difference in the security self-efficacy of freshmen and senior Cybersecurity students.

$H_0$2: There is no statistically significant difference in the security self-efficacy of female and male college Cybersecurity students.

Participants

Participants for the study consist of college freshmen and senior, female and male Cybersecurity students. Cybersecurity students are considered as anyone who is studying the security of or how to secure an information system. This includes smart phones and cellular network components, local and wide area network components, software applications, the Internet and World Wide Web, social media; along with any electronic component or software, that transfers data. Female and male students from only freshmen and senior classes were allowed to participate in the study. Freshmen students were chosen for the study as they presumably have little, formalized training or experience in the field of Cybersecurity. Senior students were chosen for the study as they have received formalized training and experience in the field of Cybersecurity. These four groups provide appropriate samples of individuals with little training and experience and those who have it.

It should be noted that threats to the internal validity of the study could include previous exposure to Cybersecurity threat identification and mitigation. Younger students are considered digital natives; people who have been exposed to technology all their lives (Christensen, 2012). Being exposed to technology over a lifetime, students may have experienced cyber threats and learned protection/mitigation mechanisms and procedures that influence their security self-efficacy. Extensive and formalized training is not common and was presumed to unlikely affect

security self-efficacy to a high degree. External validity was assured by limiting the study to Cybersecurity students within the college.

The age of the students was not documented, as participation was governed by grade level and gender only. Study participants were required attend college either full or part time and be on campus students as opposed to online. Employment status was not a consideration of this study. Students were required to self-identify whether they were a freshman/senior or female/male. No other personal information was collected during the research.

Study participants were located at a small, university and enrolled in an undergraduate status. Their involvement in the study was on a voluntary basis with an initial announcement about the study from their professors and in classroom flyers and notifications from their professors. Each professor delivered announcements for study participation approximately one week prior to the survey availability. Details of the study were provided to the professors and Department Head two weeks prior to the survey availability. Students from five classes took part in the survey with a sample size of 33 student participants. Each class consists of 15-18 students on average.

Setting

The setting for the research was at a small university in South Carolina and consisted of student participants enrolled in the school's Cybersecurity programs. The study concept was initially introduced within the Universities' classes by each class's professor. The actual research utilized an online survey that was administered via the Internet and accessible via any Internet capable device. Cybersecurity professors provided each student with verbal and written, detailed instructions containing a link to the online survey. Students were provided with an opportunity to ask clarification questions before they begin. Students had the opportunity to take

the surveys at the end of each class and professors will provided twenty minutes of in-class time to complete them. Students could also opt to take the survey on their own time and in an environment of their choosing. Surveys were assessable by electronic means such as a laptop, smart phone, tablet, or the colleges Internet assessable computers. Before the survey could be completed, the students were required to acknowledge via an electronic consent form that they are participating on a voluntary basis and their participation in no way had a bearing on the grade they made in the class. The students also acknowledge that the college in which they attend was not sponsoring the study. Other than gender identification, personal identifiable information was not be collected during the survey.

Instrumentation

The instrumentation in this study utilizes principles found within the Protection Motivation Theory (PMT) created by Dr. R.W. Rodgers in 1975 (MacDonell et al., 2013). PMT is founded on the basis of human fears such as smoking (Rogers, 1983). If an individual were to smoke for an extended period of time, the likelihood of them getting Cancer would increase. Likewise, in the event that a person was to dawn a blindfold and run onto the highway during a high traffic time, the probability of them getting hit by a car would increase. By having these fears, people can be motivated to do or accomplish certain things such as not smoke or run out in traffic blindly.

The PMT can be used to predict an individual's intentions to engage in protective actions (Anderson and Agarwall, 2010). If there are threats to an information system, the likelihood of that individual to engage in threat mitigation can be determined. This construct can be broken down into greater detail. Not only can their intentions be determined, so can their self-efficacy to mitigate the perceived threat.

Utilizing Threat and Coping Appraisals, the PMT model is applicable to Cybersecurity (MacDonell et al., 2013). Threat Appraisals (TA) assesses the severity and seriousness of a situation. Coping Appraisals (CA) determine how the situation will be responded to. To effectively use CA, they must be broken down into two categories, efficacy and self-efficacy (MacDonell et al., 2013). Efficacy is the expectancy that following recommendations eliminates the threat while self-efficacy is the belief in one's self to effectively carry out the recommendations to eliminate a threat (Rogers, 1983).

The PMT model historically has been used to examine one threat and mitigation procedure at a time, however Crossler and Bélanger (2014) have developed a Unified Security Practices (USP) instrument that examines a multi-tiered approach to Cybersecurity with great success. Like the USP, this instrument takes into account multiple security practices, not just one and can therefore look at security as a whole. By looking at Cybersecurity in a more all-encompassing manner, one's overall self-efficacy toward it can be determined based on principles found in the PMT and USP. The instrument consists of a twenty-question survey that can be administered on-line or in paper form. Multiple aspects of validity were address in the creation of the instrument. Content and face validity were addressed specifically by creating initial survey questions and submitted to multiple university researchers and reviewed with comments as well as posted on the SYSLIB University of Florida library listserv server (Phelps, 2005). After reviewing comments, the survey was revamped to accommodate the peer review. After the pre-test of the instrument, it was then revised and converted to a web based survey for a pilot test and broader review of non-Floridian Liberians utilizing SYSLIB and revised once again (Phelps, 2005). The survey was then mailed out to participants. On response analysis of the survey additional revisions were made. Predictive validity resulted in a Chi-square = 86.957,

(11df), p=.0000 (Phelps, 2005). Construct validity, the ability of the instrument to measure hypothetical constructs was based on one's direct and indirect experience task initiation and security task experience and utilized a Likert scale for measurement (Phelps, 2005). Specific security self-efficacy questions were derived from an expert group and tasking from the Computer Emergency Response Team (CERT) (Phelps, 2005). Utilizing Chronbach's alpha, the reliability was measured to be an acceptable 0.9423 (Phelps, 2005). Phelps (2005) has adapted the instrument to meet self-efficacy standards of measurements put fourth by Compeau and Higgins (1995b). When measuring the results, one's self-efficacy can be measured and compared to other group participants.

Procedures

This study commenced with the identification of one college with multiple Computer Science/Cybersecurity programs that had the potential to yield at least a 30-person sample group. Obtaining authorization or approval from the Institutional Review Board (IRB) was a crucial step in getting the study started. IRB approval was sought from both the researcher's academic institution as well as the student participant's local university. Once approval was granted from both academic institutions, the researcher worked with the local university Computer Science Department Head to organize on-site efforts. At that point, classes were identified in which to recruit study participants and inform professors of the researcher's intent. Professor contact information for each target survey participant group was identified and used to approach them via their Department Head by phone and email with the details of the study. They were provided with specific instructions as how to implement the survey used for data collection. High-level instructions, processes and procedures, methods, web pages, timelines, and training materials were provided to the university as appropriate. Refer to Appendix A.

Survey questions utilize principles found in both the Protection Motivation Theory by (Rogers, 1983) and the Technology Threat Avoidance Theory by (Laing & Xue, 2009). It was administered via web-based capabilities and assessable with any web-enabled device. The professors were asked to inform their class at least one week prior to the survey and ascertain an approximate number or participants and report that information to the researcher. They were asked to allow students to use the last twenty minutes of class to complete the survey. Results of the online surveys were immediately available to the researcher for processing via the on-line survey tool. Once received, the data was then be entered into SPSS Statistical software and analyzed. The statistical test used was a one-way ANOVA. All assumptions and criteria were met and interpretation of the data took place and included within the research study.

Data Analysis

Data analysis determined the means of four groups for comparison thus requiring a one-way ANOVA statistical test. The use of a one-way ANOVA was further justified as the groups are naturally occurring and were not exposed to any treatments introduced by the researcher. When the ANOVA was chosen, six preliminary assumptions were met. The first assumption of a dependent variable being measures at a continuous level was been met (Laerd, 2015). The second assumption of one independent variable consisting of two or more categorical, independent groups was also met (Laerd, 2015). The independent variable of Cybersecurity students was broken down into four groups consisting of freshmen, seniors, females and males. The third assumption of independence of observations was met in that all group participants are independent of the other groups (Laerd, 2015). The study was conducted with the assumptions of no outliers, a normally distributed dependent variable, and homogeneity of variance all being

assumed (Laerd, 2015). Post hoc testing was not expected to be necessary. Effect size was expected to be determined. The study was broken down into the following:

Actions and Variables

1. Compare the security self-efficacy (DV) of freshmen (IV) and senior (IV) Cybersecurity Students.
2. Compare the security self-efficacy (DV) of female and male Cybersecurity Students.

Groups

1. Group 1 – Freshmen (Independent Variable)
2. Group 2 – Seniors (IV)
3. Group 3 – Females (IV)
4. Group 4 – Males (IV)
5. Self-efficacy – (Dependent Variable)

The one-way ANOVA was to test the null hypothesis that examines the amount of security self-efficacy in college Cybersecurity students. The ANOVA required the assumptions of normality and homogeneity of variance was affirmed. The group size was not greater than 50 so the Kolmogorov-Smirnov Test for Normality was not employed. The Shapiro-Wilks test of normality was used due to a group size of less than 50. A 95% Confidence Interval was also utilized.

Using Phelps (2005) self-efficacy instrument, researchers were able to identify Cybersecurity student's self-efficacy. This information was based on security practices as a whole, which provide an accurate measure of one's attitude towards their ability to identify and defend against threats in direct relation to a multi-faceted security defense mechanism. By comparing freshmen/senior and female/male security self-efficacy, educators may have the

opportunity to tailor Cybersecurity programs to effectively meet the challenges of an ever-changing world of information systems and technology.

CHAPTER FOUR: FINDINGS

Overview

The purpose of this study is to determine if there is a difference in the security self-efficacy of freshmen and senior, female and male undergraduate Cybersecurity students. Examining the security self-efficacy of these students will enable educators to better determine each group's security posture and therefore provide a substantive framework to develop appropriate curriculum to meet the educational needs of those students. The statistical analysis performed for the study was a one-way ANOVA with all assumptions being met. Due to the small participant number of this study, less than fifty, no post ad-hoc testing was conducted. Additional tests confirmed there were no outliers, data were normally distributed and homogeneity of variance was achieved. The participant group consisted of 33 students from a small, southern university. Once the tests were completed, the analysis showed that there is no significance between freshman and seniors, female and male Cybersecurity students. The Null Hypothesis one (1) was, supported. Null Hypothesis two (2) was also, supported.

Research Questions

The two research questions were the primary foundation for this study seeking to determine if there is a difference in the security self-efficacy of college freshmen and seniors, females and males who are Cybersecurity students. The research questions are as follows:

RQ1: Is there a statistically significant difference in the security self-efficacy of college freshmen and seniors Cybersecurity students?

RQ2: Is there a statistically significant difference in the security self-efficacy of female and male college Cybersecurity students?

Null Hypothesizes

$H_0$1: There is no statistically significant difference in the security self-efficacy of freshmen and senior Cybersecurity students.

$H_0$2: There is no statistically significant difference in the security self-efficacy of female and male college Cybersecurity students.

Descriptive Statistics

In order to establish a test group to conduct the analysis, students at a small, southern university randomly volunteered to participate in a Cybersecurity, self-efficacy survey. Comparisons were made between the four groups, freshmen and seniors, female and male students, thus satisfying the assumption of independence of observation. The dependent variable (Cybersecurity self-efficacy) for all participants in each group was then measured. This measurement was based on each student's confidence level to effectively respond to twenty, Cybersecurity related tasks. These levels were categorized as "confident" "moderately confident", or "very confident" with a score of 10, 20, or 30 points respectively. All responses were tallied and each participant was then assigned a score in order to measure the dependent variable.

Table 1

Descriptives

Self_Efficacy Score

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
Freshman	10	354.00	106.16	33.57	278.05	429.94	210.00	550.00
Senior	23	391.30	112.90	23.54	342.47	440.12	230.00	600.00
Total	33	380.00	110.62	19.25	340.77	419.22	210.00	600.00

Table 1: Freshman and Senior Descriptives

On inspection of the statistical Descriptives (n = 10, M = 354.00, SD = 106.16), for freshman and (n = 23, M = 391.30, SD = 112.90), for seniors in that order.

Table 2

Descriptives

Self_Efficacy Score

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
Female	11	361.81	124.40	37.50	278.24	445.39	240.00	580.00
Male	22	385.00	105.05	22.39	338.42	431.57	210.00	600.00
Total	33	377.27	110.46	19.22	338.10	416.44	210.00	600.00

Table 2: Female and Male Descriptives

On inspection of the statistical Descriptives (n = 11, M = 361.81, SD = 124.40), for female and (n = 22, M = 385.00, SD = 105.05), for males in that order.

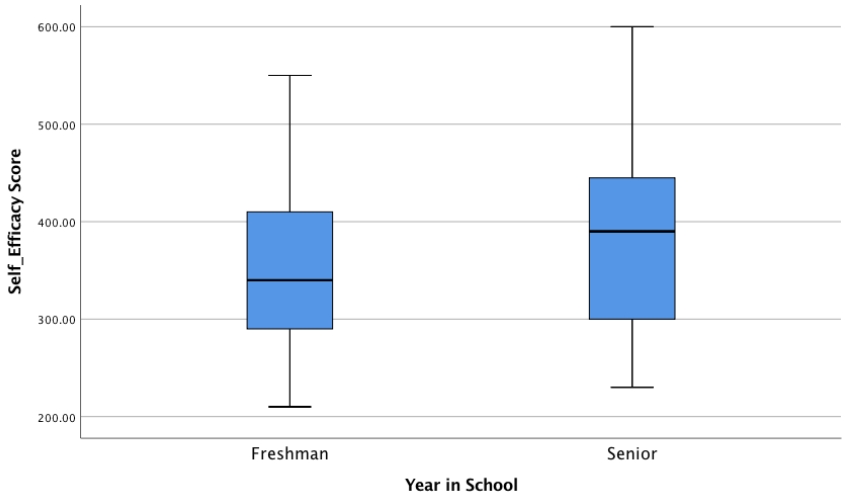

Figure 1. **Freshman and Senior Boxplot**

On inspection of the boxplot in Figure 1 there were no outliers in the assessed data for values greater than 1.5 box lengths from the box edge for the freshman and senior independent variables.

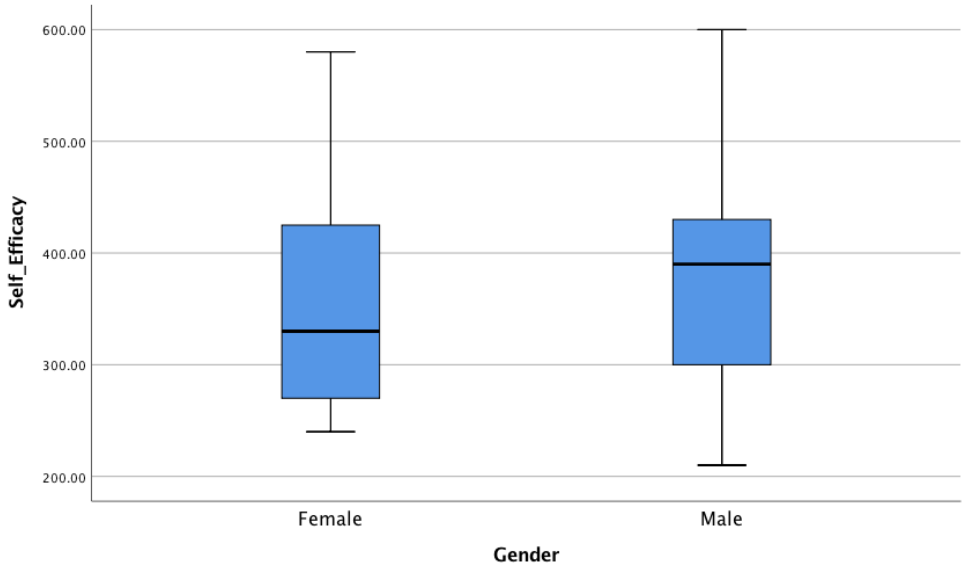

Figure 2. **Female and Male Boxplot**

Results

Hypothesis

Due to a small sample size of <50 participants, the Shapiro-Wilks test of normality was chosen to determine if data were normally distributed for the freshman and senior, female and male groups; p >.05. As shown in Table 3, data were normally distributed for the freshman and senior groups.

Table 3

Tests of Normality

	Year in School	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
		Statistic	df	Sig.	Statistic	df	Sig.
Self_Efficacy Score	Freshman	.194	10	.200*	.954	10	.717
	Senior	.105	23	.200*	.943	23	.208

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Table 3: Freshman and Senior Test of Normality

Cybersecurity self-efficacy scores were normally distributed for freshman and senior students as assessed by Shapiro-Wilk's test ($p > .05$).

Table 4

Tests of Normality

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Gender	Statistic	df	Sig.	Statistic	df	Sig.
Self_Efficacy	Female	.206	11	.200*	.857	11	.053
	Male	.107	22	.200*	.973	22	.771

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Table 4: Female and Male Test of Normality

Cybersecurity self-efficacy scores were normally distributed for female and male students as assessed by Shapiro-Wilk's test ($p > .05$).

Table 5

Test of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
Self_Efficacy Score	Based on Mean	.044	1	31	.835
	Based on Median	.042	1	31	.839
	Based on Median and with adjusted df	.042	1	30.589	.839
	Based on trimmed mean	.044	1	31	.836

Table 5: Freshman and Senior Homogeneity of Variance

Based on Levene's tests, equal variances are presence and the assumption of homogeneity of variance is met and has not been violated. Levene's test for equality of variance is (p = .835). It is **NOT** statistically significant which supports the Null Hypothesis. The assumption of homogeneity of variances has been met.

Table 6

Test of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
Self_Efficacy	Based on Mean	.510	1	31	.480
	Based on Median	.142	1	31	.709
	Based on Median and with adjusted df	.142	1	28.017	.709
	Based on trimmed mean	.411	1	31	.526

Table 6: Female and Male Homogeneity of Variance

Based on Levene's tests, equal variances are presence and the assumption of homogeneity of variance is met and has not been violated. Levene's test for equality of variance is (p = .480). It is **NOT** statistically significant which supports the Null Hypothesis. The assumption of homogeneity of variances has been met.

Table 7

ANOVA

Self_Efficacy Score

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	9699.130	1	9699.130	.787	.382
Within Groups	381900.870	31	12319.383		
Total	391600.000	32			

Table 7: Freshman and Senior ANOVA

Being that $p > .05$, there were no statistically significant differences in Cybersecurity self-efficacy scores between Freshman and Senior groups, $F(1, 31) = .787$, $p = .382$.

Table 8

ANOVA

Self_Efficacy

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	3940.909	1	3940.909	.316	.578
Within Groups	386513.636	31	12468.182		
Total	390454.545	32			

Table 8: Female and Male ANOVA

Being that $p > .05$, there were no statistically significant differences in Cybersecurity self-efficacy scores between Female and Male groups, $F(1, 31) = .316$, $p = .578$.

Table 9

Tests of Between-Subjects Effects

Dependent Variable: Self_Efficacy Score

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	9699.130[a]	1	9699.130	.787	.382	.025
Intercept	3871517.312	1	3871517.312	314.262	.000	.910
Group	9699.130	1	9699.130	.787	.382	.025
Error	381900.870	31	12319.383			
Total	5156800.000	33				
Corrected Total	391600.000	32				

a. R Squared = .025 (Adjusted R Squared = -.007)

Table 9: Freshman and Senior Tests of Between Subjects Effects

A one-way ANOVA was conducted to determine if there was a difference in the Cybersecurity self-efficacy of freshman and senior students. Participants were classified into two groups, freshman (n = 10), and senior (n = 23). Cybersecurity self-efficacy increased from freshman (m = 354.00), to senior (m = 391.30). There were no outliers, as assessed by boxplot; data was normally distributed for each group, as assessed by Shapiro-Wilk test ($p > .05$); and there was homogeneity of variances, as assessed by Levene's test of homogeneity of variances (p = .835). Differences between the freshman and senior groups was **not statistically significant**, $F(1, 31) = .787$, p = .382

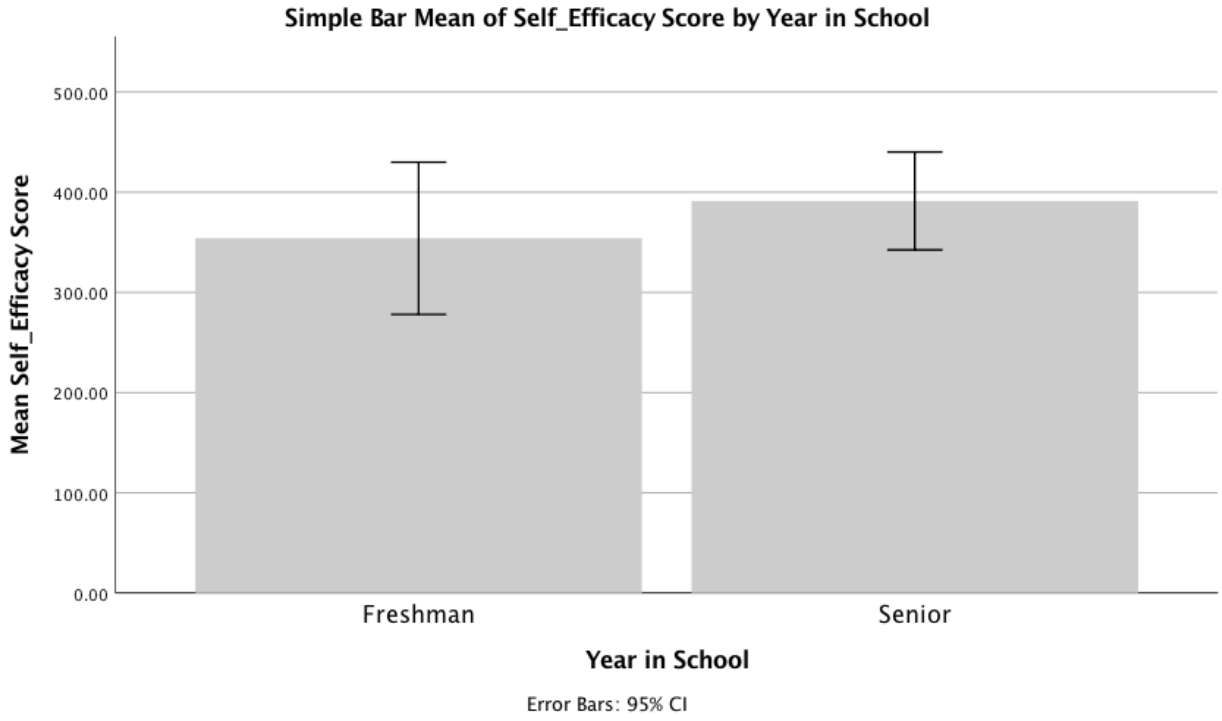

Figure 3: **Bar Mean of Self-Efficacy by Year in School**

Table 10

Tests of Between-Subjects Effects

Dependent Variable: Self_Efficacy

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	3940.909[a]	1	3940.909	.316	.578	.010
Intercept	4090074.242	1	4090074.242	328.041	.000	.914
Group	3940.909	1	3940.909	.316	.578	.010
Error	386513.636	31	12468.182			
Total	5087500.000	33				
Corrected Total	390454.545	32				

a. R Squared = .010 (Adjusted R Squared = -.022)

Table 10: Female and Male Tests of Between Subjects Effects

A one-way ANOVA was conducted to determine if there was a difference in the Cybersecurity self-efficacy of female and male students. Participants were classified into two groups, female (n = 11), and male (n = 22). Cybersecurity self-efficacy increased from female (m = 361.81), to male (m = 385.00). There were no outliers, as assessed by boxplot; data was normally distributed for each group, as assessed by Shapiro-Wilk test ($p > .05$); and there was homogeneity of variances, as assessed by Levene's test of homogeneity of variances (p = .480). Differences between the female and male groups was **not statistically significant**, $F(1, 31) = .316$, p = .578.

Hypothesis

The group means were not significantly different ($p > .05$) and, therefore, the null hypothesis cannot be rejected and the alternative hypothesis cannot be accepted.

Figure 4: **Bar Mean of Self-Efficacy by Gender**

CHAPTER FIVE: CONCLUSIONS

Overview

Self-efficacy has been shown to influence one's actions and have a primary bearing on how one will handle a particular situation or choose a certain path in life (Honicke & Broadbent, 2016). This study sought to determine if there was a difference in the Cybersecurity self-efficacy of freshman and senior, female and male students. The result of this research produced an exact agreement of the null hypothesis reflecting there was no difference between the four groups. As such, this opens the door for additional studies to determine why there was no difference as well as what influence current Cybersecurity curriculum has on the student group's Cybersecurity self-efficacy. It also presents an opportunity to develop Cybersecurity self-efficacy instruments that correctly align with and accurately reflect current, established and developing areas of technology such as social engineering, artificial intelligence, and preemptive cyber-attacks. Additional research should also be conducted to include a larger participant group so that a broader perspective can be taken into account when determining one's Cybersecurity self-efficacy.

Discussion

The purpose of this study was to determine if there is a difference between freshmen and senior, female and male Cybersecurity student's self-efficacy. Once the analysis was conducted to either accept or reject the null hypothesis, a proper determination could later be made to identify where a possible difference, if any, between the four groups existed by conducting additional research and tests. As such, in the quest to identify if there was indeed a difference, two research questions were identified and served as a basis for the study:

RQ1: Is there a statistically significant difference in the security self-efficacy of college freshmen and seniors Cybersecurity students?

RQ2: Is there a statistically significant difference in the security self-efficacy of female and male college Cybersecurity students?

Subsequently a null hypotheses for each question was developed that scrutinized each independent variable in order to identify a possible difference between the four groups. The two hypotheses are as follows:

$H_0$1: There is no statistically significant difference in the security self-efficacy of freshmen and senior Cybersecurity students.

$H_0$2: There is no statistically significant difference in the security self-efficacy of female and male college Cybersecurity students.

Both research questions aimed to address the same issues but were directed at two different groups within the Cybersecurity, academic environment. Multiple studies have been conducted to determine the self-efficacy of students from various age groups in school. Additionally, research has also been conducted to examine self-efficacy between female and male students as well. Research has also been conducted to examine the reasoning and motivation of various students in the technological arena due to self-efficacy. In a study by Mau and Li, (2018) Science, Technology, Engineer, and Math (STEM) it was identified that career aspirations and interest in those specific fields were specifically influenced by race, gender, and individual self-efficacy which resulted in a shortage of female participation in this particular instance. Self-efficacy within the STEM arena had an influence on the participation of various people groups with women as a primary focus. In the study, it was noted that female STEM students had a higher self-efficacy than their non-STEM peers who had a higher interest in a

particular area. This resulted in them actually entering the STEM program (Mau and Li, 2018). Since self-efficacy played a part in the female's decision to enter the program, one would seek to ascertain whether there is a difference between number of females and males entering the STEM arena. Similarly, the same question can be applied to the Cybersecurity self-efficacy of female and male students. Are female students with higher Cybersecurity self-efficacy entering the field of study than those who do not? Do men have a higher self-efficacy than women and enter the Cybersecurity field resulting in the offset enrollment numbers? In this study, it was noted that the overall mean of female to male independent variables Cybersecurity self-efficacy increased respectively. Although there was a slight increase in the average self-efficacy from female to males, there was no difference between the two groups. This same pattern was also present in the freshman and senior Cybersecurity self-efficacy.

Self-efficacy also has similar effects amongst high school students. Arastaman, G., & Özdemir, M. (2019) have shown that self-efficacy plays an important role in the academic aspirations of high school students. Indeed, academic self-efficacy is an important predictor of academic aspiration (Marsh & Craven, 1997). The freshman and senior participants within this study also showed a small, mean increase in Cybersecurity self-efficacy without a difference existing between the two groups.

While self-efficacy has been shown to have an influence on one's actions, there is no such indication in the participants of this study. While there is little research in the specific area of Cybersecurity self-efficacy, it is vital to know however, if there is a difference in the Cybersecurity self-efficacy of various groups. In this study, there is no difference in the independent variable groups tested and as such, until further post hoc testing is conducted, including adding additional independent variables, it is not possible to determine the extent of

each independent variable group Cybersecurity self-efficacy.

The study revealed that there was no difference in the Cybersecurity self-efficacy of freshmen and seniors. There was neither a difference in the Cybersecurity self-efficacy of female or male students. As shown by numerous studies, self-efficacy does have a direct bearing one's actions. Just as Rodgers (1975) showed with the Protection Motivation Theory, individuals will protect themselves in the event of danger. The null hypothesis was supported which is contrary to the self-efficacy influence in many areas including general technology usage. This could possibly be attributed to individual experience or the actual technological program at the university. Findings could be drastically different at a larger university with a more diverse student population.

Implications

The implications of the study have far reaching effects. As shown throughout this study, self-efficacy has a direct effect as to how people approach and handle various situations. Self-efficacy has a tremendous influence on one's actions and reactions. Regardless of the subject matter focus, one's belief in one's ability directly influences that person's path forward. The instance of Cybersecurity self-efficacy is no different than other forms. Females have been shown to enter the field of Cybersecurity at a slower rate than males yet this study has revealed there is no difference in the Cybersecurity self-efficacy of the two groups (Poster, 2018). What is the causal factor prohibiting females from entering the field? Why are males entering the field in higher numbers? Additionally, younger people use technology like never before and are very comfortable with it and often identified as digital natives. This study shows there is also no difference in the self-efficacy of freshman and senior students. In this case, are freshman so highly trained that they feel confident they can effectively handle a Cybersecurity incident or

properly secure an information system against one? Is this an instance of freshmen students not knowing what they do not know? In the case of Senior students, are they poorly trained and have a low self-efficacy? Are senior students trained so well they feel the threat is so great that they are going to have to expend a tremendous amount of skill and effort to overcome the threat, which may or may not be attainable? Research conducted at multiple universities may result in a different outcome.

Identifying there is no difference in the Cybersecurity self-efficacy between the participants in these two groups provides a substantive framework and justification for previous and current academic course evaluation along with further curriculum development. The Cybersecurity self-efficacy of female and male students was examined and the study supported the null hypothesis. As there is no difference between the two, a causal analysis should be conducted to determine why there is no difference. This can be possibly related to research by Mau and Li, (2018) which states that females within the STEM program have a higher self efficacy than those females who do not. No difference was noted between female and male students which would indicate on the surface that the current curriculum is adequate, however, were there other factors that could have possible contributed to this find? Further research should be conducted to determine if females within the Cybersecurity program supporting this research had previously participated with in a STEM at the high school or college level. Were there other programs in which female students studied that increased their self-efficacy to that of their male counterparts? Historical curriculum should be examined to determine if it is providing adequate and realistic information to the female student population. Are courses offered at the high school level presenting an appropriate representation of the Cybersecurity industry as well as the need to introduce and adequately train young students to enter the field? Examining these

courses and conducting further research will enable educators to determine their adequacy in helping to develop a student's Cybersecurity self-efficacy. It will also enable them to alter and develop new courses as student's needs and experiences change. As learning methodologies change and technology develops, these advancements can then be implemented into the academic learning process to specifically address Cybersecurity self-efficacy.

Course evaluation principle and practices can also be applied to college students. It is vital that educators continually evaluate Cybersecurity self-efficacy throughout the student's academic lifecycle. As students' progress through a traditional collegiate Cybersecurity program, it is reasonable to believe their self-efficacy should be different from when they started the program. This can be achieved through proper training, lab experience, and a general, overall knowledge of the subject matter. To help facilitate this process, multiple technological tools, applications, and teaching methodologies can be created to specifically address the self-efficacy issue.

As shown by this study, there is no difference in the Cybersecurity self-efficacy of freshman and seniors, female and male students. This is contrary to the standard effects of self-efficacy and how it has been shown to work and effect how individuals conduct themselves. As such, this would lend one to believe there is a deficiency within the Cybersecurity academic program thus resulting in no difference between freshman and seniors. Historical curriculum and other factors could also provide evidence in which to base further study into the cause of the deficiency. As the variables are expanded, a difference could possibly be observed and further testing performed to determine where exactly the difference between the groups lies between the groups. Additionally, other factors should also be identified that could possible have contributed to the identified non-difference.

Others studies have shown in limited cases that a perceived threat capability was actually not a determining factor as to how they would proceed with security mitigation implementation (Tsai, et al., 2016). The results of this study could be similar in nature in that other factors may influence the students Cybersecurity self-efficacy to address and mitigate security issues and threats. These findings warrant further investigation and a causal-comparative analysis relating to multiple independent variables.

Limitations

The limitations of this study fall directly into three categories. The first is the sample size of the study. Research was conducted at a small, southern university. Participant size for the research was limited due to the small number of students enrolled within the Computer Science program. The total participation amounted to 33, which provided very little exposure to a wide ranging and diverse student population that could have been possible at a larger university. Having a larger study participant group could possibly present differing perspectives from both the freshman and senior, female and male independent variables. Increasing the participant size would introduce a wider range of experience, which may have led to the rejection of the null hypothesis.

The second limitation of the study is that research was conducted at one educational institution, which could have produced generalized results. In the event research was conducted at multiple institutions, additional evaluation of current curriculum could have been performed yielding a greater perspective than with one study group.

The third limitation of the study was directly related to the research instrument by Phelps (Phelps, 2005). While the instrument was more than adequate to look at general information system security directly relating to Cybersecurity self-efficacy, it did not take into account

factors such as Artificial Intelligence, social engineering, espionage techniques, and automated attack systems. These are ever changing and evolving fields that have an incredible influence over Cybersecurity as a whole. Additionally, areas such as Cyber Offensive and preemptive cyber strikes were not address by the instrument. While these fields are relatively new, they are part of the everyday life in which virtual worlds operate and are key elements in the field of Cybersecurity. Whether it is personally realized or not, individuals deal with these issues every day which can possibly have an effect on their Cybersecurity self-efficacy. Further development of Cybersecurity instruments must occur in order to aid researchers and study participants alike to understand, identify, and quantify their Cybersecurity self-efficacy.

Recommendations for Future Research

Recommendations for further research abound here. An exhaustive causal-comparative analysis study of all independent variables should be conducted to determine exactly why the null hypothesis was supported for both groups. Additional research should also be focused on curriculum and its effects on Cybersecurity self-efficacy as well as an experimental study. Additional ways to enrich research in this area include:

Conduct the research across multiple educational institutions. By doing this, multiple perspectives can be examined along with varying implementations of Cybersecurity programs or majors. A direct correlation could possibly be made between a specific program of study and students within a specific academic environment.

The identification of multiple disciplines in the area of Cybersecurity and how they individually effect one's self-efficacy. Additional research in the areas of social engineering, artificial intelligence, and preemptive cyber-attacks and how they relate to one's Cybersecurity self-efficacy could be a great benefit in evaluating a student's security posture. These are areas

that Cyber professionals interact with on a daily basis and will no doubt be encountered by students and possibly have a bearing on their self-efficacy.

Course curriculum should be evaluated to determine if one's Cybersecurity self-efficacy has changed from the beginning to the end of the semester. The identification of possible changes that could be made to Cybersecurity courses will help ensure a student's self-efficacy is baselined properly and developing on par with standardized expectations.

According to Teo, (2016) there is no consensus or evidence that identifies a significant difference in the Cybersecurity self-efficacy of digital immigrants or natives. There is limited research in this field, which should be expanded. Research should focus to determine if large age differences of students significantly effect their Cybersecurity self-efficacy resulting in how they respond to security incidents relating to various information systems.

A scenario based experimental study should be conducted that would test the various independent variables ability to perform Cybersecurity tasks within a given situation. The student's reaction and self-efficacy to implement mitigation procedures could then be measured. Additionally, their actions could be assessed for accuracy, which would provide a basis for determining if the student had a high or low self-efficacy and had the ability to perform tasks correctly. This could possibly determine if the student was victim of knowing what they did not know. This experimentation could provide valuable assistance in determining the need to create realism within an entire curriculum lifecycle.

The principles of this study should be applied to the workforce in order to determine their Cybersecurity self-efficacy. One of the primary methodologies China uses to collect intellectual property is by infiltrating or compromising the desktop of company employees. This is accomplished through the use of Trojans and compromising URL links. By using the principles

of this study to evaluate an employee's Cybersecurity self-efficacy, specific training could be developed to meet occurred deficiencies resulting in a better prepared workforce that is willing, able, and confident to address security concerns.

This study had a narrow focus with limitations to freshman and senior, male and females. The study should be expanded to all students to include sophomore and juniors. Additionally, the study could be expanded to high school students, which will lend support in growing their self-efficacy and preparing them to enter collegiate Cybersecurity programs. Multiple instruments should be developed that can be reasonably adapted to new and emerging technological Cybersecurity concerns.

REFERENCES

Abawajy, J. (2014). User preference of Cybersecurity awareness delivery methods. *Behaviour & Information Technology, 33*(3), 236-248. doi:10.1080/0144929X.2012.708787.

Abomhara, M., Koien, G. M., & Department of Information and Communication Technology, University of Agder, Norway. (2015). Cybersecurity and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cybersecurity and Mobility, 4*(1), 65-88. doi:10.13052/jcsm2245-1439.414.

Anderson, C., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643. Retrieved from http://www.jstor.org/stable/25750694.

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

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304. doi:10.1016/j.chb.2014.05.046.

Arastaman, G., & Özdemir, M. (2019). Relationship between academic aspiration, academic self-efficacy and cultural capital as perceived by high school students.*Egitim Ve Bilim, 44*(197) Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu/docview/2184010163?accountid=12085.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787-2805. doi:10.1016/j.comnet.2010.05.010.

Bandura, A., & Locke, E. A. (2003). Negative self-efficacy and goal effects revisited. *Journal of Applied Psychology, 88*(1), 87-99. doi:10.1037/0021-9010.88.1.87.

Bellini, C. G. P., Isoni Filho, M. M., de Moura Junior, Pedro Jácome, & Pereira, Rita de Cássia de Faria. (2016). Self-efficacy and anxiety of digital natives in face of compulsory computer-mediated tasks: A study about digital capabilities and limitations. *Computers in Human Behavior, 59*, 49-57. doi:10.1016/j.chb.2016.01.015.

Bertino, E., Choo, K., Georgakopolous, D., & Nepal, S. (2016). Internet of things (IoT): Smart and secure service delivery. *ACM Transactions on Internet Technology (TOIT), 16*(4), 1-7. doi:10.1145/3013520.

Bertino, E., & Islam, N. (2017). Botnets and internet of things security. *Computer, 50*(2), 76-79. doi:10.1109/MC.2017.62.

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and Cybersecurity. *Security Dialogue, 44*(2), 147-164.

Bradbury, D. (2014). Unveiling the dark web. *Network Security, 2014*(4), 14. doi:10.1016/S1353-4858(14)70042-X

Bressler, M. S., & Bressler, L. (2015). Protecting your company's intellectual property assets from cyber-espionage. *Journal of Legal, Ethical and Regulatory Issues, 18*(1), 21-34. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/1693348002?accountid=12085.

Calhoun, C. D. (2017). Incorporating blended format Cybersecurity education into a community college information technology program. *Community College Journal of Research and Practice, 41*(6), 344-347. doi:10.1080/10668926.2016.1269691.

Carver, C. S., & Scheier, M. F. (1982). Control theory: A useful conceptual framework for personality-social, clinical, and health psychology. *Psychological Bulletin 92*(1), 111-135.

Cavus, N., & Ercag, E. (2016). The scale for the self-efficacy and perceptions in the safe use of the internet for teachers: The validity and reliability studies. *British Journal of Educational Technology, 47*(1), 76-90. doi:10.1111/bjet.12217.

Chen, I. (2017). Computer self-efficacy, learning performance, and the mediating role of learning engagement. *Computers in Human Behavior, 72*, 362. doi:10.1016/j.chb.2017.02.059.

Cheryan, S. (2012). Understanding the paradox in math-related fields: Why do some gender gaps remain while others do not? *Sex Roles, 66*(3), 184-190. doi:10.1007/s11199-011-0060-z.

Chrisensen, C. (2016). *Disrupting class: How disruptive innovation will change the way the world learns*. S.l.: Mcgraw-Hill Education.

Cornell, D., & Limber, S. P. (2015). Law and policy on the concept of bullying at school. *American Psychologist, 70*(4), 333-343. http://dx.doi.org.ezproxy.liberty.edu/10.1037/a0038558.

Compeau, D. R., & Higgins, C. A. (1995b). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-211.

Craig, A. N., Shackelford, S. J., & Hiller, J. S. (2015). Proactive Cybersecurity: A comparative industry and regulatory analysis. *American Business Law Journal, 52*(4), 721-787. doi:10.1111/ablj.12055.

Crossler, R., & and Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection Motivation Theory and a Unified Security Practices (USP) instrument. *SIGMIS Database, 45*(4), 51-71. http://doi=http://dx.doi.org/10.1145/2691517.2691521.

Dadkhah, M. (2015). New types of fraud in the academic world by cyber criminals. *Journal of Advanced Nursing*, , n/a. doi:10.1111/jan.12856.

Davison, C. B., & Stein, C. H. (2014). The dangers of cyberbullying. *North American Journal of Psychology, 16*(3), 595-606. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/1635437455?accountid=12085.

Dohr, A., Modre-Opsrian, R., Drobics, M., Hayn, D., & Schreier, G. (2010). The internet of things for ambient assisted living. Paper presented at the 804-809. doi:10.1109/ITNG.2010.104.

Dymond, S., Schlund, M. W., Roche, B., Houwer, J. D., & Freegard, G. P. (2012). Safe from harm: Learned, instructed, and symbolic generalization pathways of human threat-avoidance. *PLoS One, 7*(10) doi:http://dx.doi.org/10.1371/journal.pone.0047539.

Enstein, A. (n.d.). Albert Einstein Quotes. Retrieved from https://www.brainyquote.com/quotes/albert_einstein_385842.

Fitzpatrick, W. M., & Dilullo, S. A. (2015). Cyber espionage and the S.P.I.E.S. taxonomy. *Competition Forum, 13*(2), 307-336. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/1755486045?accountid=12085.

Gall, M. D., Gall, J. P., & Borg, W. R. (2015). *Applying educational research: How to read, do, and use research to solve problems of practice* (7th ed.). Boston, MA: Pearson/Allyn & Bacon.

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the dark web social network. *New Media & Society, 18*(7), 1219-1235. doi:10.1177/1461444814554900.

Gundecha, P., Barbier, G., Tang, J., & Liu, H. (2014). User vulnerability and its reduction on a social networking site. *ACM Transactions on Knowledge Discovery from Data (TKDD), 9*(2), 1-25. doi:10.1145/2630421.

Haggard, S., & Lindsay, J. R. (2015). North Korea and the Sony hack: Exporting instability through cyberspace. *Asia - Pacific Issues,* (117), 1-8. Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu/docview/1690004558?accountid=12085.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security, 4*(2), 49-60. doi:http://dx.doi.org/10.5038/1944-0472.4.2.3.

Honicke, T., & Broadbent, J. (2016). The influence of academic self-efficacy on academic performance: A systematic review. *Educational Research Review,17,* 63-84. doi:10.1016/j.edurev.2015.11.002.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks, 20*(8), 2481-2501. doi:http://dx.doi.org.ezproxy.liberty.edu/10.1007/s11276-014-0761-7.

Kang, J., Djafari Marbini, H., Patel, P., Fawcett, N., & Leaver, L. (2015). Survey of medical students' use of social media. *The Clinical Teacher, 12*(6), 373-377. doi:10.1111/tct.12320.

Khan, F. U. (2011). States rather than criminals pose a greater threat to global Cybersecurity: A critical analysis. *Strategic Studies, XXXI*(3) Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/1231703177?accountid=12085.

Kim, B. C., & Yong, W. P. (2012). Security versus convenience? An experimental study of user misperceptions of wireless internet service quality. *Decision Support Systems, 53*(1), 1–11.

Kim, E. B. (2014). Recommendations for Cybersecurity awareness training for college students. *Information Management & Computer Security, 22*(1), 115-126. doi:http://dx.doi.org/10.1108/IMCS-01-2013-0005.

Knopová, M., & Knopová, E. (2014). The third world war? in the cyberspace. Cyber warfare in the middle east. *Acta Informatica Pragensia, 3*(1), 23-32. doi:10.18267/j.aip.33.

Kruger, H. A., & Kearney, W. D. 2006. A prototype for assessing Cybersecurity awareness. *Computers and Security, 25*, 289–296.

Laerd Statistics (2015). One-way ANOVA using SPSS Statistics. *Statistical tutorials and software guides*. Retrieved from https://statistics.laerd.com/.

Lee Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems, 50*, 361–369.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71–90.

Lim, I., Park, Y., & Lee, J. (2016). Design of security training system for individual users.*Wireless Personal Communications, 90*(3), 1105-1120. doi:10.1007/s11277-016-3380-z.

MacDonell, K., Chen, X., Yan, Y., Li, F., Gong, J., Sun, H., & Stanton, B. (2013). A Protection Motivation Theory-based scale for tobacco research among Chinese youth. *Journal of Addiction Research & Therapy, 4,* 154–. http://doi.org/10.4172/2155-6105.1000154.

Mannarini, S., & Boffo, M. (2014). The relevance of security: A latent domain of attachment relationships. *Scandinavian Journal of Psychology*, *55*(1), 53-59. doi:10.1111/sjop.12091.

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*,*59*(3), 257-266. doi:10.1016/j.bushor.2016.01.002.

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), Article 2.

Marsh, H. W., & Craven, R. (1997). Academic self-concept: Beyond the dustbowl. *Handbook of Classroom Assessment: Learning, Achievement, and Adjustment*, 131-198.

Martinez, J. A., U.S.A.F., & Kayser, M. R., U.S.A.F. (2013). Cyber professionals in the military and industry-partnering in defense of the nation. *Air & Space Power Journal*, *27*(1), 4-21. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/1318929574?accountid=12085.

Mattos, C. L. (2013, May). From Rio to the world: What security managers can learn from Brazil--front line in the global cyber wars. *Software World, 44*(3), 13+. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://go.galegroup.com.ezproxy.liberty.edu:2048/ps/i.do?p=ITOF&sw=w&u=vic_liberty&v=2.1&it=r&id=GALE%7CA333332652&sid=summon&asid=676085f7b5d731a32ab958f5a215fcd7.

Mau, W. J., & Li, J. (2018). Factors influencing STEM career aspirations of underrepresented high school students. *The Career Development Quarterly, 66*(3), 246-258. doi:http://dx.doi.org.ezproxy.liberty.edu/10.1002/cdq.12146.

Mensch, S., & Wilkie, L. (2011). Cybersecurity activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal, 14*(2), 91-116. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/886806258?accountid=12085.

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy & Security, 9*(1), 47-67. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/1350244208?accountid=12085.

Mejias, R. J., & Balthazard, P. A. (2014). A model of Cybersecurity awareness for assessing Cybersecurity risk for emerging technologies. *Journal of Information Privacy & Security, 10*(4), 160-185. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/1691007767?accountid=12085.

Mejias, R. J., & Harvey, M. (2012). A case for Cybersecurity awareness programs to protect global information, innovation and knowledge resources. *International Journal of Transitions and Innovation Systems, 2,* 302–324.

Mohsen Nia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things.*IEEE Transactions on Emerging Topics in Computing, ,* 1-1. doi:10.1109/TETC.2016.2606384.

Moin, U., Zarka, Z., & Karuna, S. (2016). Challenges in privacy and security in banking sector and related countermeasures. *International Journal of Computer Applications, 144*(3), 24-35.

Moore, G. E. (n.d.). Moore's Law. Retrieved from http://www.mooreslaw.org/.

Morgan, S. (2015). The business of Cybersecurity: 2015 market size, cyber crime, employment, and industry statistics. Retrieved from http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/2/#721844894e68 .

Nolin, J., Olson, N., Högskolan i Borås, & Akademin för bibliotek, information, pedagogik och IT. (2016). The internet of things and convenience. *Internet Research, 26*(2), 360-376. doi:10.1108/IntR-03-2014-0082.

O'Kane, P., Sezer, S., & McLaughlin, K. (2011). Obfuscation: The hidden malware. *IEEE Security & Privacy, 9*(5), 41-47. doi:10.1109/MSP.2011.98

Hacktivists.

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials, 16*(1), 414-454. doi:10.1109/SURV.2013.042313.00197.

Pfleeger, S. L., & Caputo, D. D. (2012). *Leveraging behavioral science to mitigate cyber-security risk*. MITRE Technical Report 12-0499. Bedford, MA: MITRE Corporation.

Phelps, D. C. (2005). *Information system security: Self-efficacy and security effectiveness in Florida libraries.*

Poster, W. R. (2018). Cybersecurity needs women. *Nature*, *555*(7697), 577. Retrieved from http://link.galegroup.com.ezproxy.liberty.edu/apps/doc/A572639598/SCIC?u=vic_liberty&sid=SCIC&xid=02971a63.

Radisavljevic-Gajic, V., Park, S., & Chasaki, D. (2018). Vulnerabilities of Control Systems in Internet of Things Applications. *IEEE Internet of Things Journal,5*(2), 1023-1032. doi:10.1109/jiot.2017.2787962.

Rizzo, B. (2016). Data of 200 million yahoo users for sale on the dark web. *Database and Network Journal*, *46*(4), 13.

Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social Psychophysiology. New York: Guilford Press.

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? In L. F. Cranor, & S. Garfinkel (Eds.), Security and Usability: Designing secure systems that people can use (pp. 13e30). Sebastopol: O'Reilly. This needs converting to APA.

Saxena, P., Kotiyal, B., & Goudar, R. H. (2012). A cyber era approach for building awareness in Cybersecurity for educational system in India. *International Journal of Information and Education Technology*, *2*(2), 167. doi:http://dx.doi.org/10.7763/IJIET.2012.V2.102.

Schnackenberg, H. L., Vega, E. S., & Simard, D. A. (2014). Paradigm shift: Introduction of a social media network and Web 2.0 technology into a college classroom environment. *Journal of Cases on Information Technology, 16*(2), 1+. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://go.galegroup.com.ezproxy.liberty.edu:2048/ps/i.do?id=GALE%7CA383575380&sid=summon&v=2.1&u=vic_liberty&it=r&p=AONE&sw=w&asid=258a8343f46a15b3b5ca0b6128866f5e.

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national Cybersecurity strategies. *International Journal of Computer Science and Information Security, 14*(1), 129-136. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/1764183576?accountid=12085.

Shields, K. (2015). Cybersecurity: Recognizing the risk and protecting against attacks. *North Carolina Banking Institute, 19,* 345.

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

Slusky, L., & Partow-Navid, P. (2012). Students Cybersecurity practices and awareness. *Journal of Information Privacy & Security, 8*(4), 3-26. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/1318750219?accountid=12085.

Smith, C., & Kumar, A. (2018). Crypto-Currencies – An introduction to not-so-funny moneys. *Journal of Economic Surveys, 32*(5), 1531-1559. doi:10.1111/joes.12289.

Spalevic, Z., & Ilic, M. (2017). the use of dark web for the purpose of illegal activity spreading. *Ekonomika, 63*(1), 73. doi:10.5937/ekonomika1701073S.

Surry, D. W., & Baker, F. W. (2016). The co-dependent relationship of technology and communities. *British Journal of Educational Technology, 47*(1), 13-28. doi:10.1111/bjet.12349.

Tait, A. (2017, February 23). 10 Internet of Things Security Vulnerabilities. Retrieved September 23, 2017, from http://blog.learningtree.com/10-internet-of-things-security-vulnerabilities/.

Tamrin, S. I., Norman, A. A., & Hamid, S. (2017). Information systems security practices in social software applications. *Aslib Journal of Information Management,69*(2), 131-157. doi:10.1108/ajim-08-2016-0124.

Teo, T. (2016). Do digital natives differ by computer self-efficacy and experience? an empirical study. *Interactive Learning Environments, 24*(7), 1725-1739. doi:10.1080/10494820.2015.1041408.

Thompson, R. E. (2016). Cybersecurity: Getting proactive about data vulnerability. *Florida Bar Journal, 90*(1), 36.

Tolmie, P., & Crabtree, A. (2018). The practical politics of sharing personal data. *Personal and Ubiquitous Computing, 22*(2), 293-315. doi:http://dx.doi.org.ezproxy.liberty.edu/10.1007/s00779-017-1071-8.

Tsai, S.H., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., & Cotton, S.R. (2016). Understanding online safety behaviors: A Protection Motivation Theory perspective. *Computers & Security*, *59*, 138-150, doi:http://dx.doi.org/10.1016/j.cose.2016.02.009.

Warikoo, A. (2013). Cyber warfare China's role and challenge to the United states. *Himalayan and Central Asian Studies, 17*(3), 61-0_4. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/1470421358?accountid=12085.

Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism, 39*(3), 195-206. doi:10.1080/1057610X.2015.1119546.

Weiser, M. (1993). Ubiquitous computing. *Computer, 26*(10), 71.

What is Bitcoin? (n.d.). Retrieved September 24, 2017, from http://money.cnn.com/infographic/technology/what-is-bitcoin/.

Wiener-Bronner, D. (2014). Report shows cyber crime is on the rise. Retrieved from http://www.thewire.com/technology/2014/04/report-shows-cyber-espionage-is-on-the-rise/361024/.

Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication, 1*(4), 317-342.

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. doi:10.1016/j.chb.2008.04.005.

Zhang, K., Liang, X., Lu, R., & Shen, X. (2014). Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal, 1*(5), 372-383. doi:10.1109/JIOT.2014.2344013.

Appendix A

Instructions

One Week Before the Survey

Professors: Tell your students they will have an opportunity to participate in an online Cybersecurity survey. Its purpose is to compare the security self-efficacy of freshmen and senior, female and male Cybersecurity students. Participation is voluntary and will not affect their grade in the class. It takes about twenty minutes to complete and will be given during class. The survey will help researchers determine if there is a difference in freshmen and senior, female and male Cybersecurity student's security self-efficacy. Do students feel there is a Cybersecurity threat and are they prepared to meet that threat and effectively protect information systems against it? Ultimately, the study will help researchers identify differences in self-efficacy and potentially fill in any gaps that may be present.

Day of the Survey

Professors: Allow your students twenty minutes to complete the following survey at the end of your classes. Read the following instructions to your students:

Students: The following survey compares the security self-efficacy of freshmen and senior, female and male Cybersecurity students. You may complete it on your smart phone or the schools computers. It consists of thirty questions and can be found at www.thislink.com. You have twenty minutes to complete it. Please answer every question. If you have technical difficulties, please let me know and you will be provided another opportunity to take the survey. Answer all the questions honestly and completely. Your participation in this survey will not affect your grade. If you do not want to participate in the survey, you do not have to but must

remain in the classroom until the end of the regularly scheduled class time. Please do not share or compare answers. You may begin now.

Appendix B

IRB Approval

LIBERTY UNIVERSITY.
INSTITUTIONAL REVIEW BOARD

October 5, 2018

Lane H. Melton
IRB Exemption 3185.100518: Comparing the Sense of Security Self-Efficacy Amongst College Freshmen and Senior, Female and Male Cyber Security Students

Dear Lane H. Melton,

The Liberty University Institutional Review Board has reviewed your application in accordance with the Office for Human Research Protections (OHRP) and Food and Drug Administration (FDA) regulations and finds your study to be exempt from further IRB review. This means you may begin your research with the data safeguarding methods mentioned in your approved application, and no further IRB oversight is required.

Your study falls under exemption category 46.101(b)(2), which identifies specific situations in which human participants research is exempt from the policy set forth in 45 CFR 46:101(b):

> (2) Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless:
> (i) information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

Please note that this exemption only applies to your current research application, and any changes to your protocol must be reported to the Liberty IRB for verification of continued exemption status. You may report these changes by submitting a change in protocol form or a new application to the IRB and referencing the above IRB Exemption number.

If you have any questions about this exemption or need assistance in determining whether possible changes to your protocol would change your exemption status, please email us at irb@liberty.edu.

Sincerely,

G. Michele Baker, MA, CIP
Administrative Chair of Institutional Research
The Graduate School

LIBERTY
UNIVERSITY.
Liberty University | Training Champions for Christ since 1971