

**College of Professional Studies**

Social Engineering Susceptibility: A Study on Demographics and Information Security Awareness in Small Businesses

by

Amy Hetro Washo

Submitted in Partial Fulfillment of the Requirements for the Degree of

Ph.D. in Strategic Leadership and Administrative Studies

December 2019

**Committee Chair:** Dr. Alan Levine

**Committee Member:** Dr. Art Comstock

**Committee Member:** Mr. Marc Gonzalez

**Reader**: Dr. Amy Paciej-Woodruff

**Reader**: Dr. Chris Speicher

**Acknowledgements**

This research and dissertation defense is dedicated in loving memory of my triplet sons, John, Elijah, and Andrew, who were with me briefly on this Ph.D. journey, but whose presence and love is felt every day. They provided the inspiration to continue my education and the motivation to try my best to make them proud of me.

Thank you to my savior, Jesus Christ, for providing me the opportunity to continue my education and be surrounded by His love and the love of others especially during the times when it was needed most. To God be all the glory.

Thank you to my dissertation committee members, Dr. Art Comstock, Mr. Marc Gonzalez, and especially to my dissertation chair, Dr. Alan Levine, whose direction, encouragement, and patience with my many questions throughout this project were invaluable to its completion. I could not have asked for a better group of people to guide me in this process. Thanks also to my readers, Dr. Chris Speicher and Dr. Amy Paciej-Woodruff, for devoting their time to reviewing my work, attending my presentation, and providing feedback.

Thank you to my family, especially my mom, Mary Claire, dad, John, and sister, Leah, who have always encouraged me in my education and every other aspect of life. I also must thank my other family members including Delaney, Oliver, Opie, and Arabelle.

And finally, the biggest thank you to my husband, Jason, for his constant love and support and always being with me through life’s good times and its challenges. We are expecting our fourth son at the time of this writing, and I couldn’t imagine going through life with anyone else by my side.

**Table of Contents**

**List of Figures and Tables** 7

**Abstract** 9

**Chapter I. Introduction**

Introduction 11

Establishing the Problem 11

Key Findings from Literature 14

Deficiencies in the Literature 16

Theoretical Framework 18

Conceptual Framework 27

Purpose Statement 29

Research Question 30

Subproblems 30

Research Hypothesis 31

Definitions 31

Delimitations 33

Significance of Study 34

**Chapter II. Literature Review**

Cialdini’s Principles of Persuasion 38

Demographics as a Determinant of Social Engineering Susceptibility 41

Gender 41

Age 43

Training 44

Cultural Identity 44

Other Variables 45

Small Business 46

Human Aspects of Information Security Questionnaire (HAIS-Q) 47

Literature Review Conclusion 51

**Chapter III. Methodology**

Research Design 53

Sample 53

Instrumentation 55

HAIS-Q 55

Demographic Data Collection 59

Procedures 60

Analysis of Data 62

Supplemental Analysis 62

**Chapter IV. Results**

Subproblems 1 – 9 64

Subproblem 10 70

HAIS-Q 70

Multiple Regression 71

Supplemental Analysis 73

Respondent Answers 73

Correlations – Knowledge, Attitude, and Behavior 77

Demographics as Predictors of Knowledge, Attitude,

and Behavior Scores 78

Knowledge, Attitude, and Behavior Scores as Predictors 82

Gender 85

Age 86

Length of Employment 86

Education 88

Weekly Hours Worked 90

Industry 91

Training 92

Training Recode 95

Rank 98

Cultural Identity 99

**Chapter V. Discussion**

Summary 101

Discussion 102

Implications 105

Limitations 109

Future Research 111

Conclusion 115

**References** 116

**Appendices**

Appendix A. Business Owner / Employee Recruitment Letter 128

Appendix B. Informed Consent Form 129

Appendix C. HAIS-Q 131

Appendix D. Demographic Survey Questions 135

Appendix E. Frequency Distribution – Participants’ Age 137

Appendix F. Frequency Distributions – Knowledge, Attitude, &

Behavior Scores 139

Appendix G. Frequency Distributions – Information Security Awareness

Scores and Susceptibility Scores 142

Appendix H. Mean & Standard Deviation of Knowledge, Attitude,

Behavior, and Susceptibility Scores by Industry 146

**List of Figures and Tables**

*Figure Name Page Number*

1 Cialdini’s Principles of Persuasion 20

2 NCCIC Cybersecurity Framework 27

3 Conceptual Framework Diagram 29

4 Modified HAIS-Q Scoring 59

*Table Name Page Number*

1 Frequency Distribution of Gender 65

2 Frequency Distribution of Education 65

3 Frequency Distribution of Length of Employment 66

3.1 Frequency Distribution of Length of Employment Recoded 66

4 Frequency Distribution of Training 67

4.1 Frequency Distribution of Training Recoded 67

5 Frequency Distribution of Industry 68

5.1 Frequency Distribution of Industry Recoded 68

6 Frequency Distribution of Rank 69

7 Frequency Distribution of Cultural Identity 69

7.1 Frequency Distribution of Cultural Identity Recoded 69

8 Multivariate Regression– Research Question 72

9 HAIS-Q Responses 74

10 Multivariate Regression – Demographics & Knowledge Score 79

11 Multivariate Regression – Demographics & Attitude Score 81

12 Multivariate Regression – Demographics & Behavior Score 82

13 Multivariate Regression – Knowledge & Attitude Scores 83

14 Multivariate Regression – Attitude & Behavior Scores 84

15 Multivariate Regression – Knowledge / Attitude & Behavior Scores 84

16 Knowledge Score – Mean & Standard Deviation – Employment 87

17 Attitude Score – Mean & Standard Deviation – Employment 87

18 Behavior Score – Mean & Standard Deviation – Employment 88

19 Susceptibility Score – Mean & Standard Deviation – Employment 88

20 Knowledge Score – Mean & Standard Deviation – Education 89

21 Attitude Score – Mean & Standard Deviation – Education 89

22 Behavior Score – Mean & Standard Deviation – Education 90

23 Susceptibility Score – Mean & Standard Deviation – Education 90

24 Knowledge Score – Mean & Standard Deviation – Training 93

25 Attitude Score – Mean & Standard Deviation – Training 93

26 Behavior Score – Mean & Standard Deviation – Training 94

27 Susceptibility Score – Mean & Standard Deviation – Training 95

28 Knowledge Score – Mean & Standard Deviation – Training Recode 96

29 Attitude Score – Mean & Standard Deviation – Training Recode 96

30 Behavior Score – Mean & Standard Deviation – Training Recode 97

31 Susceptibility Score – Mean & Standard Deviation – Training Recode 98

**Abstract**

**Introduction**: The purpose of this research was to explore the relationship between demographic characteristics and social engineering susceptibility of employees in small businesses in Northeastern Pennsylvania. The research question was: How do demographic characteristics, including gender, age, education, length of employment with a company, hours worked, industry, training, rank, and cultural identity, of employees in small businesses in Northeastern Pennsylvania predict social engineering susceptibility? **Methods:** The Human Aspects of Information Security Questionnaire (HAIS-Q) was utilized to calculate an awareness score for each participant. This awareness score was converted to a susceptibility score. Quantitative analysis including multiple regression was used to determine if any of the demographic characteristics of employees were significant in predicting social engineering susceptibility. The sample consisted of 95 small business owners and employees in Northeastern Pennsylvania, and data was collected over an eight week period. Supplemental analysis explored the demographic characteristics and whether they were significant predictors of knowledge, attitude, and behavior scores as part of the HAIS-Q. The knowledge, attitude, and behavior scores were examined to determine whether they were significant predictors of each other. **Results:** None of the demographic characteristics were significant predictors of susceptibility to social engineering. However, further exploration of the training variable determined that there was a significant difference in knowledge scores and susceptibility scores between employees who had no training and employees who had training more than three times on average in one year. In addition, knowledge was found to be a significant predictor of attitude, attitude was found to be a significant predictor of behavior, and both knowledge and attitude were found to be significant predictors of behavior. **Conclusion:** Demographic characteristics might not be as crucial in determining small business owners’ and employees’ susceptibility to social engineering. However, awareness training, while not considered a predictor of social engineering susceptibility, does have a key role in helping to mitigate social engineering attempts.

**Chapter I**

**The Problem and Its Setting**

**Introduction**

Businesses of all types and sizes are facing an unprecedented threat to the data they utilize and store in the natural course of their operations. Hackers and others who are not authorized to access this information are using sophisticated techniques to work their way into organizations by a variety of methods including social engineering. This type of hacking technique has been identified as the most widely used method (Ashford, 2016) and considered one of the leading threats to information security today (Mitnick & Simon, 2002; Airehrour, Nair, & Madanian, 2018).

Social engineering can be defined as the act of manipulating human beings, most often with the use of psychological persuasion, to obtain unauthorized access to systems containing data, documents, and general information that the social engineer should not have access to (Mitnick & Simon, 2002; Tetri & Vuorinen, 2013; Heartfield & Loukas, 2015). Social engineering today mostly focuses on the information security realm and the potential threats that face both large and small businesses as well as individuals.

**Establishing the Problem / Concern / Issue**

The study of social engineering drastically increased in the early 2000s because of the widespread use of technology to protect confidential data and the understanding that psychological manipulation, a form of non-technical hacking, could be used alone or in conjunction with technical hacking methods to obtain access to information (Abawajy, 2014; Stewart & Jurjens, 2017). Information security is a widely investigated and accepted field of study. Social engineering can be viewed as a segment of this broader topic and one that is not as well-known or researched as other divisions of information security. It is generally understood that the protection of confidential information has always been an important concept in many industries including government and business. However, considering the widespread use of technology in almost every aspect of business and personal life, and the significant value placed on confidential data, the threat of someone using any means possible to obtain that information is real and it is growing (Mitnick & Simon, 2002).

Several reasons can be given for the lack of understanding around social engineering. It is a fairly new phenomenon meaning that the published research is not as extensive as other fields. Social engineering also revolves around the human aspect of information security. Human beings are complex with fluctuating needs and emotions, and the countless interactions people have with each other every day are all opportunities for a social engineering attack to occur. Extending this discussion into the business realm, companies today operate on a global scale and their interactions with other businesses, customers, vendors, and society in general are multiplied when compared to that which occurs for a single individual. Human behavior is also broadly unpredictable. It is a challenge to anticipate an individual’s actions based on all of the factors and circumstances that affect behavior (Elifoglu, Abel, & Tasseven, 2018).

Most companies spend a significant amount of money on systems-based protections but often do not devote time to understanding the human element of information security (Lineberry, 2007). Yet, if employee behavior is overlooked, ignored, and not considered an essential component in an organization’s information technology structure, the most technically secure systems in the world cannot compete against the human beings that must operate, program, or utilize them (Mitnick & Simon, 2002). An employee, sometimes referred to as an insider, can cause damages that significantly outweigh those inflicted from an outside party (Elifoglu et al., 2018; Unintentional Insider Threats, 2014).

Social engineering can be referred to as soft hacking, meaning that hackers do not necessarily have to break into or disrupt a system. Instead, they use the human element, also identified as the weakest link in information security, to gain unauthorized access (Mitnick & Simon, 2002; Goel, Williams & Dincelli, 2017; Aleem, Wakefield, & Button, 2013). For example, rather than intrusively accessing a system, the social engineer makes a phone call or sends an email, posing as someone else, and asks for the information. People tend to share a lot of information if they are simply asked (Mitnick & Simon, 2002).

The interconnectedness of today’s world is one of the catalysts for social engineering occurrences that can impact every individual who has a bank account, a loan, a social security number, or a paycheck. If someone has a unique identifier that remains private to the individual, it is almost a guarantee that someone would like to get access to that information (Mitnick & Simon, 2002). Businesses can also be victims of social engineering, and they pose even more of a hazard because of the far-reaching impacts a social engineering attack can have on them. When a business faces a social engineering threat, the number of people that can be impacted is unlimited. Employees, investors, and clients of the company might have confidential data compromised leading to lack of trust, termination of the business relationship, or loss of assets. The major industries in today’s world including financial, healthcare, government, and insurance can be targets for social engineers trying to obtain data or access that they should not have (FSB, 2016).

Systems protections are certainly helpful to mitigate some social engineering attacks, but they are not enough. What if the person accessing the system has the right to access the information, and merely shares it over the phone or sends it in an email to someone who is thought to hold the same access credentials? A system protection can do little to diminish an attack like this. The Federal Bureau of Investigation’s internet crime complaint center cites the increased use of social engineering and business email compromise (BEC) schemes which have resulted in billions of dollars in losses over the past several years (FBI, 2018).

**Key Findings from Literature**

Experts in the field have identified the human element as the weakest link in the entire information security realm (Mitnick & Simon, 2002; Goel et al., 2017; Aleem et al., 2013). Those tasked with information security in organizations almost always have some level of protection for the computer systems, but the threats facing organizations today are what experts would call a converged threat. This description means that the threats come from a variety of sources and have a variety of aims, sometimes on the systems and other times on the individuals operating the systems. It is often a combination of both. The converged threat makes the study of social engineering difficult because it does not arise from one unique source and have one main impact. This distinction explains the need for an integrated approach to examine the complex subject of social engineering (Elifoglu et al., 2018).

Many of the published studies in information technology journals explain the subject of protecting information in terms of a psychological and a financial perspective (Ifinedo, 2016; Anderson, Baskerville, & Kaul, 2017; Aleem et al., 2013). This conclusion is further confirmation that understanding the impacts of social engineering cannot exclusively be found in one field. Rather, the disciplines rely on each other to essentially fill in the gaps where each one is lacking.

The social engineering literature has an extensive focus on psychological concepts. One of the key elements used in social engineering is persuasion and several researchers have used key characteristics of persuasion (Cialdini, 2007) in their studies that are essential to an attack (Bullee, Montoya, Pieters, Junger, & Hartel, 2015; Bullee et al., 2018; Komatsu, Takagi, & Takemura, 2013; Muscanell, Guadagno, & Murphy, 2014; Butavicius, Parsons, Pattinson, McCormac, 2015). They include reciprocation, commitment, social proof, liking, authority, and scarcity (Cialdini, 2007). The various influences are based on qualities found in the victim, but are used on behalf of the attacker to exploit a psychological trait leading to the desired access.

Turning their attention to practical protections that can be used in organizations today, researchers use the psychological concepts mentioned previously as a guide on how an information security department should be built and how it should function in an organization (Parsons et al., 2015). Never before has there been such a strong emphasis placed on the psychological aspect of information technology and how companies use their knowledge of human behavior to mitigate social engineering attacks (Carlton & Levy, 2017; Bullee et al., 2018; Elifoglu et al., 2018; Dawson & Thompson, 2018; Hsu, Lee, & Straub, 2012). The trend in information security is viewing it as more of an administrative issue compared to a technological one meaning equal emphasis is being placed on the human, managerial, and clerical side of an organization and not just on systems protections (Hsu et al., 2012).

The prior research studies have been helpful in focusing attention on the psychological composition of an employee base in organizations and determining if any of the qualities present in employees can be used to predict whether an employee will fall victim to a social engineering attack. However, psychological characteristics can change depending on an individual’s life circumstances. For example, a social entry point (Tetri & Vuroinen, 2013) such as trust or greed is not always present in human beings. An employee’s level of trust or feelings of greed can change depending on many of the basic demographic characteristics that this research will study such as age and education. Demographic qualities are more consistent, do not change as rapidly as psychological states, and could perhaps be the precursor to why people exhibit those characteristics (Salerno & Peter-Hagene, 2015).

**Deficiencies in the Literature**

Some deficiencies have been found in past literature which have helped to guide this research study. In terms of data collection, caution should be used when interpreting the results of prior research studies that had admitted flawed methodology (Stewart & Jurjens, 2017), small sample size (Bullee et al., 2018; Abawajy, 2014), and narrow population focus (Workman, 2007; Bullee et al., 2018).

Most of the studies on social engineering or related types of information security attacks have been conducted on a confined and isolated group such as university faculty, employees, and students in one particular class, department, or campus (Jansson & vonSolms, 2013; Vishwanath, Herath, Chen, Wang, & Rao, 2011; Wright, Chakraborty, Basoglu, & Marett, 2010; Van Kleef, van den Berg, & Heerdink, 2015; Snyman & Kruger, 2016; Zheng et al., 2018; Vishwanath, Harrison, & Ng, 2016) or employees in one department or company (Workman, 2007; Pattinson, Butavicius, Parsons, McCormac, & Calic, 2017; Halevi, Memon, & Nov, 2015). It can be difficult to draw generalizations based on a homogenous group of individuals, but if caution is used, the information in those studies can still provide insight into the topic of social engineering and can be used as the foundation for other studies.

Another deficiency in the research can be found in the populations studied. Few studies have been done on small businesses, defined here as entities with less than 25 employees. It can be argued that these businesses are likely targets for social engineers since they might think that their size makes them less of a target (Social-Engineer, 2018). Small businesses often work with a limited staff meaning that one person might perform multiple functions and have unrestricted access to systems, information, and buildings (FSB, 2016). Also, smaller businesses are less likely to have the funding in a budget for social engineering trainings or protections that could help mitigate risks (Jackson, 2018).

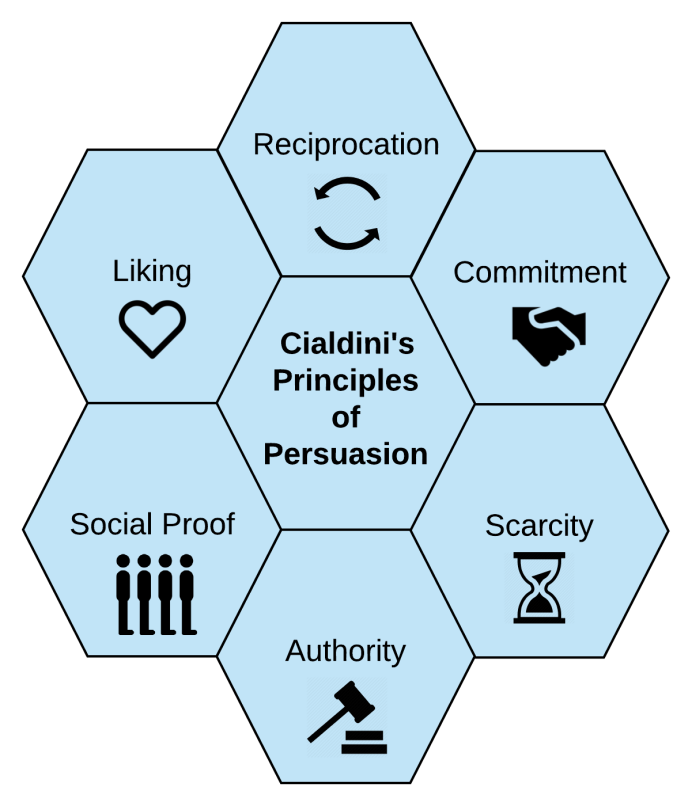
There are over 30 million small businesses in the United States as defined by the U.S. Small Business Administration, and they comprise over 99% of all businesses in the United States (SBA.gov, 2018). The statistics further support the need to study the concept of social engineering and how it affects the majority of businesses in the United States. Small businesses know that they need to protect themselves from the impending threats to information security, but there is little information in the research that provides practical options for them to utilize. The need to conduct research of this type is certainly prevalent in today’s business world. A survey by Hiscox (2018) reported that 66% of small business have identified concerns related to cybersecurity, and yet less than one third of those businesses engaged in training against phishing scams, one type of social engineering attack, and almost half do not have an employee devoted to cyber protection (Hiscox, 2018).

The research problem to be addressed in this study is the susceptibility to social engineering of employees in small (less than 25 employees) businesses. The human element is really the main focus for social engineering studies. Understanding how basic employee demographics could highlight potential weaknesses in an organization’s information security structure and help to guide the organization to implement security controls and protections that would work best with their employee populations. Demographics such as gender, age, education, length of employment with a company, hours worked, industry, training, rank, and cultural identity can serve as independent variables since they are thought to possibly impact social engineering (Airehrour et al., 2018; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). The independent variables can be studied to explore the relationship to the dependent variable, susceptibility to social engineering, and whether they can be used to predict it.

**Theoretical Framework**

Psychological theories guide many of the studies on social engineering by providing a framework within which to view the intricacies of the subject. Prior research has used systems theory to help understand the groups and subsystems that comprise an organization, both formally and informally, and identify where there are gaps in the security framework (Young & Leveson, 2014; Ritzman & Kahle-Piasecki, 2016). After all, organizations consist of complex relationships and alliances, and it is critical for managers to understand how these networks impact information security (Nekoranec, 2013). Bullee et al. (2015) and van Bavel, Rodriguez-Priego, Vila, & Briggs (2019) discuss the application of protection motivation theory to describe behavior related to information security. This theory suggests that fear appeals contain multiple components and affect the response of individuals to these appeals. The components include the extent of the event, how likely it is that the event will occur, and the perception of the individual’s response (Rogers, 1975). Bullee et al. (2015), Goel et al. (2017), Van Kleef et al. (2015), Komatsu, Takagi, & Takemura (2013), and Moody, Galletta, & Dunn (2017) have noted the use of the Elaboration Likelihood Model of persuasion proposed by Petty and Cacioppo (1981). This model helps to explain the effective communication between sender and receiver and how messages can be used as a form of persuasion.

Several researchers (Bullee et al., 2015; Bullee et al., 2018; Muscanell et al., 2014) have studied the principles of persuasion as identified by Cialdini (2007). Tetri & Vuorinen (2013) are critical of the application of Ciadini’s principles of persuasion to the information security field suggesting that it is difficult to view the principles in that type of environment. However, social engineering attacks do not occur in isolation and solely within the realm of information security. Rather, they take place in the typical, social workplace environment with all the complexities of various people, systems, and multiple factors impacting the attack itself and the success of it. It is logical then to apply the principles of persuasion to a variety of environments, anytime persuasion is used to convince someone to do something.



*Figure 1.* Cialdini’s six principles of persuasion. This figure illustrates the principles outlined by Cialdini that are used in persuasive situations (2007).

*Image has been added by the researcher*.

Cialdini (2007) proposed six principles of persuasion that can be used in a variety of fields such as business, sales, politics, and even in personal relationships such as with a spouse or when raising children. He initially explains the concept of fixed-action patterns derived from the study of animals in their natural environment. Human beings also exhibit a similar process of fixed patterns of behaviors without much thought given to those behaviors. This automatic behavior serves an appropriate function in people’s lives by allowing individuals to make quick decisions for daily repetitive choices and react quickly when a situation requires an immediate response. People sometimes do not have the time or capability to analyze every aspect of their situation which makes the fixed-action patterns important. There exists a trigger mechanism that prompts a response or an action, but sometimes the triggers incite the fixed-action behavior at an inappropriate time. It can be easy for someone to manipulate one of the triggers and trick someone into an action that would not have been taken if the person analyzed the situation rather than relying on the fixed-action pattern that he or she was accustomed to.

This type of manipulation is at the core of social engineering attacks and is relied on heavily by the attacker, knowing that the victim will likely react in a pre-established way when faced with a request. The six principles of persuasion are used by social engineers as they construct the setting, word choice, and mode of communication used to hopefully lead to a successful attack, one in which data, access, or sometimes both are freely given to the attacker.

The first principle outlined by Cialdini (2007) is reciprocation which is the act of providing something in return to someone who has done a favor for the person. Cialdini (2007) provides a reciprocation example in which people feel obligated to give a birthday gift to someone who has given a gift to them. Adherence to the unwritten reciprocity rule is found in almost every culture which makes it a highly successful form of persuasion. In fact, even a small favor done for someone has been shown to be met with an equal or even bigger favor in return. This idea is so convincing to individuals because of their inherent need to be accepted and liked by society. Since it is an expectation in almost every culture that a favor be returned, people may think that society, or their immediate sub-set of it, will not look favorably on them if they do not adhere to this rule. Applying this principle to social engineering suggests that the attackers may have a higher probability of a successful attack if they first offer the potential victim a small gift or perform a small gesture. In return, the victim feels obligated to provide the information or access required by the social engineer.

The second principle is commitment and consistency. Human beings have a penchant for standing by decisions they have made even when contrary evidence supports they are wrong. It essentially has a snowball effect in that individuals will continue to make decisions based on that earlier, and sometimes wrong, decision. Sticking with a previous choice reflects consistency which is a highly sought characteristic in people. The idea that human beings cannot process all of the information available or think through appropriate behavior in every situation further supports the significance of consistency. It ensures that individuals will not think about their actions; rather, they will just act consistently with prior behavioral patterns. If the social engineers can make the victim commit to something, then they can rely on the consistency of the behaviors that follow the commitment. This consistency and eventual lack of thinking on behalf of the victim have a high potential of leading to a successful attack.

Social proof can be considered the third principle of persuasion as defined by Cialdini (2007). This concept supports the idea that people determine what is correct based on what others think. This is especially true in uncertain times when most people will look at the actions and behaviors of others to determine their own ways of acting. Even more specifically, individuals tend to model their behavior or respond favorably to those who are similar to them. This principle has major implications for social engineering. The attackers might be much more persuasive if they can convince the victim that by complying with their request, the victim is acting similarly to everyone else. The idea of social proof encourages certain types of behavior and permits individuals to act in such a way that they feel they fit in socially with those around them. Even if people question their behavior in terms of what everyone else is doing, they often assume that other people must have more information or knowledge on the subject so behaving in that way, even though it may inherently seem wrong, will suddenly become more apparent and seem like the right thing to do. Watering hole attacks are a type of social engineering technique that capitalizes on social proof. Rather than targeting an individual, the attacker targets a social platform in which people collectively tend to visit based on similar characteristics. An example of this would be the targeting of a website that provides industry-wide regulations, knowing that the collective employee base of one company would likely visit that site (Watering Hole, 2017).

The fourth principle is liking which means that people who wish to influence or persuade will usually try to convince others to like them. Attractive people are usually associated with favorable characteristics whether or not they actually exist in the individual. In addition, people tend to like others they are comparable to in terms of a similar upbringing, the same hobbies and interests, or matching opinions. Human beings also are inclined to fall for flattery whether it be honest or insincere. Cialdini cites an “automatic positive reaction” to flattery which distorts our observation and thinking about a certain situation (2007). The more that an individual likes someone, the more influence that person is able to exert. A social engineer can use many of the concepts associated with this principle of liking to ensure a successful attack. It benefits the attackers to convince the victim to like them, compliment the victim, and show proof, whether real or fake, that they are similar in some way.

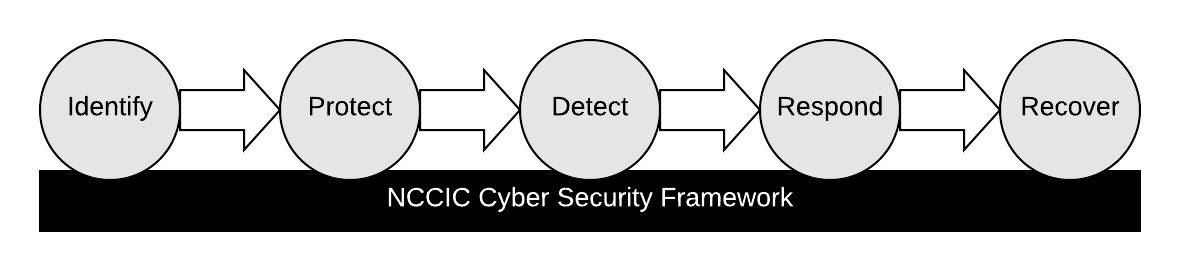
Authority is the fifth principle and the one most often used in social engineering attacks (Bullee et al., 2018). Adherence to authority is common in many cultures, and people are expected to behave in ways that respect and obey authoritative figures. This behavior provides advantages on a societal level to ensure order and reduce chaos, and it is usually ingrained in most people that this is common behavior. Similar to the commitment and consistency principle, authority is another means of providing a guide for behavior and thoughts when there is just too much information to process and determine how to act. Authority provides an immediate and automatic response and compliance to requests since it is assumed that those in positions of power have more knowledge and control. The use of titles and clothing choice can provide visual clues as to who has power, and even more specifically, the extent of that power. Social engineers can mimic authority figures by dressing a certain way and introducing themselves with a prestigious or authoritative title. In most situations, this persuasion technique diminishes the chance for the victim to question the request and more importantly, encourages him to comply with it.

The last principle of persuasion is scarcity which means that a limited or diminishing quantity of something, be it a product, time, or individual, makes it more enticing to a person. The threat of losing something is a strong motivator especially when viewed in terms of limiting people’s freedoms. By removing choices, the opportunity to decide among many options is taken away and as a result, it causes people to cling to those options, ensuring that they will continue to have access to them. Limitless and unceasing options do little to influence a person since they are missing the element of scarcity. Things also become more desirable if people must compete against each other for it. Social engineers can use this tactic to influence a potential victim by explaining what can be lost if the individual does not comply with the request. Denial of the request can be explained to correlate with limiting opportunities for an individual, making that person cling more tightly to whatever freedoms he may be enjoying. In order to not have freedoms taken away, the victim may decide to comply with the request.

As applied to this study, the principles of persuasion supported the idea that the independent variables including demographic characteristics could possibly influence susceptibility to social engineering based on how each of the demographic measures responds to the principle used in the social engineering attack. Cialdini (2007) proposed that people use the available information around them to make decisions especially in times of stress or uncertainty; however, only a small amount of that information is utilized by individuals because of the inadequate capacity to comprehend everything or because of limited time. There is so much knowledge surrounding people, more than ever before, that human beings are forced to rely on cues in the environment to tell them how to act and respond. Social engineers have found ways to manipulate these cues, and this study will examine individual behavior in response to cues used in conjunction with the principles of persuasion. The research study aimed to determine if there is a significant difference in the way that employees respond to environmental cues which would have an effect on their susceptibility to social engineering.

Persuasion principles were used in conjunction with the cybersecurity framework as provided by the National Cybersecurity and Communications Integration Center (NCCIC) from the United States Department of Homeland Security to guide the research. A perspective on influence and persuasion helps to analyze the psychological aspects inherent in social engineering attacks. When combined with a professional, practical model, the two perspectives provided a solid framework to guide the research in this study.

This cybersecurity framework was initially created as a guide for organizations to protect themselves from cybersecurity threats. There are five functional areas included in this framework. The first is *Identify* and provides the foundation on which the other areas will be built upon. It explains the need for organizations to assess their risks in the operational environment. They should understand the systems, processes, and other resources utilized in their environment, the risks from both an inherent and external view, and their assessment and governance policies. The second area is *Protect* and involves the deployment of protections to guard against intrusions to any of the components identified in the first functional area. The third area is *Detect* and encompasses the efforts of exposing a cybersecurity attack. This functional area should not only be concerned about an attack that has already occurred, but also the events that led up to it and a process for continuous observation. The fourth area is *Respond* and involves the reaction to a cybersecurity attack. Responses can include physical actions, communication, and analyzing the attack. The fifth and final area is *Recover* and involves the strategies utilized to maintain resilience in the organization. The plans in this area should include how to recapture any lost functionality that occurred during the attack and how future events can be mitigated (NCCIC, Cybersecurity Framework).



*Figure 2.* NCCIC cybersecurity framework. This figure outlines the five functional areas of the framework suggested to increase cyber resilience in organizations.

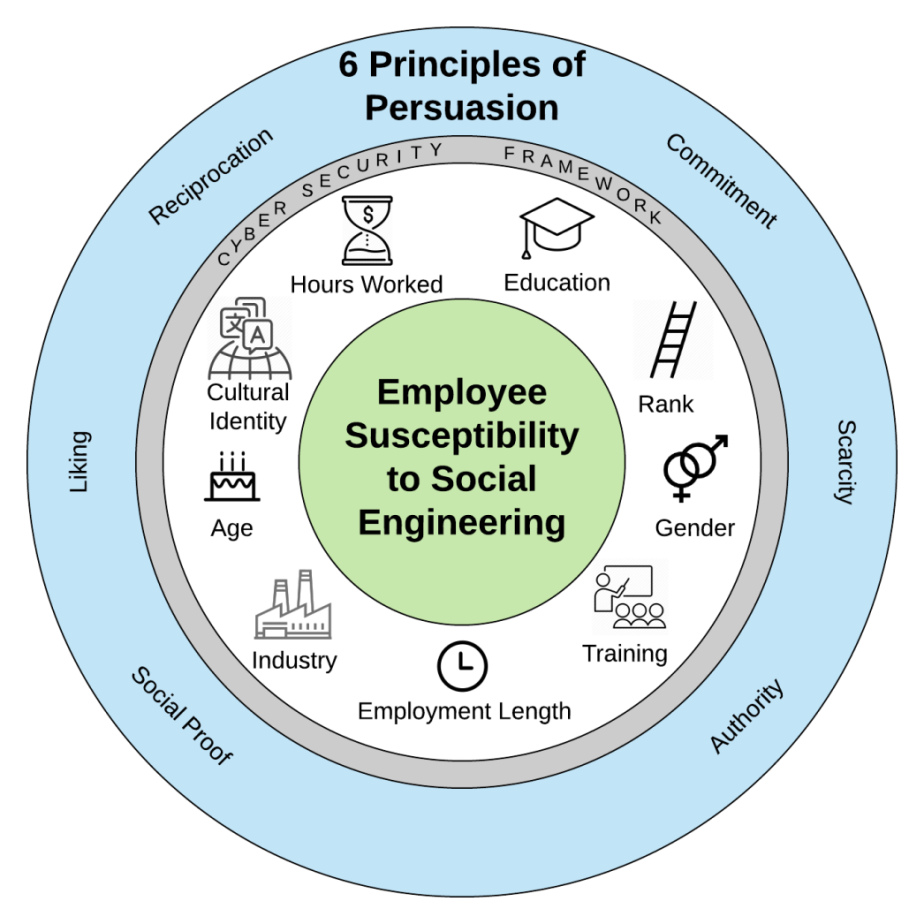
*Image has been added by the researcher*.

The intention of the Cybersecurity Framework is for it to be used as a means of cyber resilience in organizations. Resiliency in cyberattacks means becoming less susceptible to social engineering and the ability to recover and continue business operations after a social engineering attack occurs. The effectiveness of persuasion on the demographic characteristics can be increased or decreased depending on the strength of the Cybersecurity Framework, and as a result, employee susceptibility can also increase or decrease. The principles of persuasion and this framework guided the research and served as a solid model, one that predicates and follows this study respectively. This particular framework from the United States Department of Homeland Security was chosen based on the quality reputation of this governmental organization and the ease of implementation in small businesses to help protect themselves from cyberattacks and improve their cyber resilience.

**Conceptual Framework**

The conceptual framework for this research study utilized the six principles of persuasion as identified by Cialdini (2007) including reciprocation, commitment, social proof, liking, authority, and scarcity. Either one, some, or all of the principles are utilized as the underlying force in all social engineering attacks. The principles impact employees to various extents, perhaps based on certain demographic characteristics such as gender, age, education, length of employment with a company, hours worked, industry, training, rank, and cultural identity. The degree to which employees are influenced by the principles are possibly based on demographic characteristics and relate to that employee’s susceptibility to social engineering.

The Cybersecurity Framework as provided by the United States Department of Homeland Security can be implemented in organizations today as a safeguard between the principles of persuasion and the employee base in organizations. The framework can be modified based on the organization’s particular needs, composition of employees based on demographic features, and other factors in the internal and external environment that may impact information security.

****

*Figure 3*. Employee susceptibility to social engineering. This figure shows how the six principles of persuasion outlined by Cialdini (2007) influence responses based on employee demographics and as a result, also impact susceptibility to social engineering.

*Image has been added by the researcher*.

**Purpose Statement**

The purpose of this study was to examine the relationship between demographic characteristics and susceptibility to social engineering of small business employees working in various industries in northeastern Pennsylvania in the United States. The demographic characteristics include gender, age, education, length of employment with a company, hours worked, industry, training, rank, and cultural identity. Susceptibility to social engineering was captured as a self-report measure using the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).

**Research Question**

How do demographic characteristics, including gender, age, education, length of employment with a company, hours worked, industry, training, rank, and cultural identity, of employees in small businesses in northeastern Pennsylvania predict social engineering susceptibility?

**Subproblems**

The sub-problems addressed in this research study include the following:

What is the gender of participants?

What is the age of participants?

What is the length of employment of participants?

What is the education level of participants?

What is the average number of hours worked per week of participants?

What is the industry of the participants?

What information security / social engineering training have the participants had?

What is the rank of the participants?

What is the cultural identity of the participants?

How do demographic characteristics of the participants predict social engineering susceptibility?

**Research Hypothesis**

**Null Hypothesis.**

The demographic characteristics of employees in small business including age, gender, education, length of employment with a company, hours worked, industry, training, rank, and cultural identity, do not predict susceptibility to social engineering.

**Alternative Hypothesis.**

The demographic characteristics of employees in small business including age, gender, education, length of employment with a company, hours worked, industry, training, rank, and cultural identity, predict susceptibility to social engineering.

**Definitions**

The demographic characteristics serve as the independent variables in this study and can be explained in the following ways.

* Gender can be defined as male, female, or other.
* Age is the numerical measurement of years a person has been alive.
* Education can be defined as the level of formal instruction received by the employee including various levels of secondary and higher education.
* Length of employment with a company is defined by the number of years the individual has worked for the company he/she is currently working for, regardless of whether the person’s position or hours worked have changed.
* Hours worked can be defined as how many hours per week an employee works.
* Industry can be defined as a “distinct group of productive or profit-making enterprise” (Merriam-Webster.com). In this study, it will be measured by question # 8 which provides the following list of industries for an employee to choose: healthcare, marketing, construction, technology, nonprofit, law, finance, insurance, other.
* Training can be measured as the number of times per year the employee received training or education on cybersecurity awareness.
* Rank can be defined as whether one identifies as owner / highest ranking official or non-owner / non-highest ranking official of the company.
* Cultural identity can be defined as the ethnic background in which the participants identify most closely with in terms of language, religion, traditions, and values (Race and Ethnicity, Psychology Today, n.d.).
* Employee can be defined as a person who works at a particular organization and receives compensation in return for work efforts.
* Small business can be defined as an entity that is in existence to solve a problem or meet the needs of customers and employs less than 25 people.
* Northeastern Pennsylvania can be further clarified as the geographic region of the northeastern section of the state of Pennsylvania.
* Social engineering is defined as the act of manipulating human beings, most often with the use of psychological persuasion, to obtain unauthorized access to systems containing data, documents, and general information that the social engineer should not have access to (Mitnick & Simon, 2002; Tetri & Vuorinen, 2013; Heartfield & Loukas, 2015).
* Susceptibility to social engineering can be defined as the likelihood that an individual will fall victim to a social engineering attack as a result of low information security awareness as measured on the HAIS-Q. Other research studies have analyzed social engineering susceptibility in terms of social networks like Facebook (Algani, Xu, & Chan, 2015) or phishing scams (Goel et al., 2017, Sheng et al., 2010). This study will define susceptibility in the same way as those referenced studies but will instead operationalize susceptibility based on employee information awareness as measured in the HAIS-Q.

**Delimitations**

The researcher has restricted this study to the population of small businesses located in northeastern Pennsylvania in the United States. It can be difficult to draw generalizations from a small geographic region and apply the findings industry-wide. However, the results of this study provided a solid foundation that further research can be built upon, perhaps in other geographic locations or within a single industry.

Only individuals with company email addresses had the opportunity to participate in the study. The population excluded a large group of employees that could arguably be susceptible to social engineering attempts but could not be measured with this type of research tool. This limitation can be addressed in future research studies using a different mechanism to capture employee responses.

The number of variables that could impact social engineering is limitless. The researcher chose the demographic characteristics that she believes were the most important to the study with the understanding that there are additional factors that could influence social engineering susceptibility. Similarly, other dependent variables rather than susceptibility could be measured based on the collection of the employee demographic information. These additional factors could be included in future research studies.

**Significance of Study**

The research study described here is significant in terms of studying a growing threat to information security as well as studying it in the context of small businesses. Few research studies have been done on this population even though it is the most common type of business in the United States (SBA.gov, 2018). Small businesses are comprised of employees who often perform multiple roles, perhaps with little separation of duties, and know each other well enough that the thought of a social engineering attack may not seem plausible to them (Social-Engineer, 2018).

The examination of demographic information of employees is important to this study because it could potentially identify factors that contribute to an organization’s susceptibility to social engineering. An organization is only as strong as the most vulnerable individual user of company systems (Abawajy, 2014). If demographic characteristics that comprise an employee base can be analyzed to determine susceptibility to social engineering, it can have major implications on how information security protocols are designed and implemented in organizations. The relationship between the variables, if any, can also guide training and development programs and help managers proactively guard against information security attacks in the form of social engineering as they perform their daily management functions in leading an organization.

Several groups could benefit from the outcomes of this research. No one is immune to social engineering so individuals and businesses of any size can gain valuable information to better understand this phenomenon and how it might impact them. Determining the relationship, if any, between employee demographics and susceptibility to social engineering can impact both the theoretical and practical realm in which social engineering is studied. Psychological theories can be applied to the results of the study to further investigate the demographic variables studied here. In an organizational setting, the results of the study could provide guidance as to how an information security program should be established, implemented, and monitored to mitigate social engineering attempts. The findings could offer additional insight into understanding the composition of employee bases in organizations and how employees can better work together to impact business outcomes. Compiling and analyzing demographic characteristics can help to decrease the success of social engineering attacks (Unintentional Insider Threats, 2014).

In the past few years, there have been several infamous social engineering attacks that disrupted business operations, financial markets, and government related agencies. In 2013, social engineers gained unauthorized access to the Twitter account for the Associated Press, and posted a fabricated story about an explosion at the White House and injury of then president Barack Obama. In the three minutes the post was active before being discovered as a hack, the Dow Jones Industrial Average dropped over 150 points which equals a market value of about $136 billion (InfoSec, 2018). In early 2016, social engineers impersonated the CEO of Snapchat and sent email requests to employees for confidential information. A simple ask via email resulted in the theft of employee data of over 700 employees of the company (Leary, 2016). Also in 2016, a laptop belonging to an employee of Premier Healthcare was stolen through social engineering techniques. The computer lacked technical safeguards and as a result, confidential health information of over 200,000 individuals was stolen. (Leary, 2016). A final example of social engineering is the 2016 attack on the United States Justice Department. The social engineer obtained access to a department employee’s email account and attempted to access a restricted web portal that required an access code. The attacker called the employee support number, posed as a new employee, and was provided the access code to the system by simply asking for it. As a result of this attack, the personal information of an estimated 20,000 FBI employees and 9,000 Justice Department employees was shared publicly. It is still unclear what additional information may have been stolen and the impact it could have on employees, the governmental departments, or society in general (InfoSec, 2018).

All of the previous examples have occurred in large companies. However, social engineering is just as much of a threat to small businesses as it is to large businesses. Often times, social engineering in small business is not well reported and not as news worthy to the general public (Social-Engineer, 2018), but there are still lesser known cases that have caused harm to or the dissolution of the business. An article published in *The Guardian* in 2010 references three examples of social engineering attacks on small businesses. The first involved a lawyer who established a company specializing in corporate training who was later forced to shut down as a result of social engineering (Smith, 2016). A technology start-up company called Skimlinks was the target of a social engineering attack in which the controller received an email from someone claiming to be a manager in the company requesting a wire transfer of funds to an account (Smith, 2016). Lastly, a small event supplies company received invoices for advertising services that were not legitimate, but they were social engineered into paying them anyway (Smith 2016).

These are just a few of the social engineering attacks that had impacts both in the United States and globally. From the examples, it is clear that social engineering can strike any organization and often times, it is merely one or a few individuals that fall victim to the attacks and cause extensive damage. The widespread use of social engineering techniques and the lack of immunity of any one person or group support the need for a research study of this type. Individuals and organizations can learn more about the nature of social engineering attacks and use the data and analysis within this study to help modify their behavior and that of others in their organizations.

**Chapter II**

**Literature Review**

A literature review was conducted of any relevant and pertinent research studies that relate to the research question being addressed in this particular study. Also included is research that relates to the theoretical framework through which this question is being viewed. Social engineering is a complex and multifaceted event that lacks both a conceptual framework (Janczewski & Fu, 2010) and a practical, real-world framework (Williams, Hinds, & Joinson, 2018) through which to study its occurrence. Several researchers have had to rely on theories and models from other disciplines to better understand the nuances contained within a social engineering attack.

**Cialdini’s Principles of Persuasion**

Cialdini’s (2007) six principles of persuasion have been utilized throughout the research and include reciprocation, commitment, social proof, liking, authority, and scarcity. Persuasion has been identified as one of the key components of social engineering. Several researchers have analyzed these principles and measured how they influence the potential victim in a social engineering attack.

Persuasion is an inherent quality of social engineering and focuses specifically on the connection between the attacker and the victim. For example, how likely is it that employees obey authority figures in their organization? Bullee et al. (2015) proposed that the use of authority would increase the likelihood that a social engineering attack would succeed. While the assumption was logical, they could not validate this hypothesis, but they attributed it to cultural differences in the power of authority. The society in the United States is built upon adherence to authority, and most people have been taught to obey authority if they are to be an upstanding member of society (Bullee et al., 2018). Similarly, this same idea can be applied in an organizational situation. Good employees are expected to obey authority whether it be a direct boss, higher-level executive, or anyone with more tenure than that employee. However, in other cultures, authority may not be viewed similarly to the United States and therefore the idea of authority as a persuasive influence may be reduced (Bullee et al., 2015).

Williams et al. (2018) found that authority and urgency used together increased the chance that recipients of a phishing email would click on a suspicious link in that email. Similarly, Butavicius et al. (2015) determined that authority was effective as a means to convince recipients of emails that those emails were safe, yet the use of social proof, another of Cialdini’s principles, was not an effective influencer. They have also identified that some of the persuasion principles such as liking, reciprocation, and consistency were difficult to study in the context of their research since those principles relate more to an ongoing relationship between the sender and recipient.

Bullee et al. (2018) conducted a study to determine whether various forms of information awareness (pamphlet, key chain, or poster) used as an intervention would mitigate the effect of authority in a planned social engineering attack. Employees not subjected to the intervention were almost three times more likely to provide the social engineer posing as a facilities manager with keys to their offices. However, the intervention did not significantly change the effect that authority had on the employees, and they attributed the cultural explanation described earlier as one of the reasons why the intervention had little to no effect on the power of authority.

An alternative example using conformity looked at how closely employees mirrored their behaviors to others in the organization (Meng & Jun, 2017). Another study analyzed how indebted people felt to do something in return for a gesture that was done for them (Happ, Melzer, & Steffgen, 2016). They determined that reciprocity is highly influential and that by giving people a small piece of chocolate, they were more likely to reveal personal, confidential information. The principle of likability was studied solely in the context of an online setting, and it was determined that it is not a significant influencer in that type of environment (Guadagno, Muscanell, Rice, & Roberts, 2013).

Workman (2007) studied Cialdini’s principles of persuasion (2007) in the context of psychological characteristics of the potential victim. He found that individuals with higher normative commitment respond well to a reciprocity tactic in which they feel indebted to another to return a favor. In addition, he found that individuals who are more trusting are likely to fall victim to an attack. Relating this to Cialdini’s principles (2007), he notes that likeability tends to be higher in people that we trust.

Uebelacker & Quiel (2014) developed a social engineering personality framework by proposing the application of Cialdini’s principles (2007) to the Five Factor Model proposed by McCrae & John (1992) which includes the traits of conscientiousness, extraversion, agreeableness, openness to experience, and neuroticism. They suggested that conscientious individuals would more likely be persuaded by authority, reciprocity, and commitment. Similarly, Halevi et al. (2015) determined that the trait of conscientiousness is highly correlated to fabricated phishing scams and their corresponding level of response. Halevi et al. (2015) also found that the characteristic of extraversion would be more likely to yield to the persuasion technique of social proof and those high in neuroticism would be less susceptible to a phishing attack.

Using these principles of persuasion and other psychological means is an important step in trying to determine an individual’s susceptibility to social engineering. Some studies have discovered certain consistent, identifiable qualities that might make employees more susceptible to becoming victims. Social engineers will prey on these social entry points (Tetri & Vuroinen, 2013) and exploit human qualities such as the fear of losing / eagerness to gain (Goel et al., 2017; Cheung-Blunden, Cropper, Panis, & Davis, 2018), likability and trust (Flores, Holm, Svensson, & Ericsson, 2013; Guadagno, et al., 2013), boredom proneness (Moody et al., 2017), or positive characteristics such as patience and kindness in addition to negative characteristics such as greed or hubris (Fan, Lwakatare, & Rong, 2017).

**Demographics as a Determinant of Social Engineering Susceptibility**

Susceptibility to social engineering is an important component of the concept. Individuals’ cognitive ability and how they process information influence their susceptibility to phishing attacks (Vishwanath et al., 2011). However, several researchers chose to study an even more rudimentary level of measuring susceptibility in individuals by analyzing their basic demographic data.

**Gender.**

Gender has been studied by multiple researchers. Several studies determined women were more susceptible to social engineering attacks than men (Sheng et al., 2010; Jagatic, Johnson, Jakobsson, & Menczer, 2007), and this includes opening phishing emails (Goel et al., 2017), responding to spear-phishing emails (Halevi et al., 2015), and using social networking websites (Algarni, Xu, & Chan, 2015). It has been suggested that men understand technology more than women so they were less likely to fall victim to a social engineering attempt in which confidential information was requested (Sheng et al., 2010). Another explanation theorizes that individuals’ emotional responses could potentially outweigh rational thinking if a characteristic of that individual is triggered by some component of the attack (Halevi et al., 2015). Depending on emotional states, employees might respond to a persuasion technique when experiencing one emotion compared to when experiencing another (Van Kleef et al., 2015).

Emotions can be a powerful influencer in changing a person’s thoughts and attitudes. In fact, the use of emotions is already widely used in politics and advertising so it makes sense that it would also be used in an organizational setting (Van Kleef et al., 2015). While it has been identified that emotions are common in organizational settings, a further distinction can be made as to whether emotions are used by males or females. Indeed, people’s perceptions of which gender displays emotion impacts the interpretation of that emotion (Salerno & Peter-Hagene, 2015). Researchers found that opinions expressed by emotional women do not influence as many people as the opinions expressed by emotional men (Salerno & Peter-Hagene, 2015). This fact relates to social engineering attackers and victims as there can now be a gender component used to determine how one can be more persuasive.

The same study also concluded that when men express anger, they are viewed as more powerful and persuasive, and in fact, even more credible than if the emotion was not present. Perhaps a male social engineer, showing anger in an appropriate situation, can convince an unsuspecting employee to provide confidential information. However, anger expressed on behalf of women was not as influential as when males used it. In the study, Salerno and Peter-Hagene (2015) found that people who viewed a woman expressing anger believed the woman to be more emotional and not persuasive in changing the views of others. These studies (Van Kleef et al., 2015; Salerno & Peter-Hagene, 2015) focused their attention on the characteristics of the source rather than the recipient but in terms of social engineering understanding, the demographic and psychological traits of both participants in the attack can help further the understanding of susceptibility to social engineering.

Continuing with studies on gender and social engineering, other researchers determined that more men than women were likely to become victims of social engineering (Happ et al., 2016) and others determined that gender was not significant in terms of predicting vulnerability to phishing scams (Moody et al, 2017). Based on these contradictory findings, further research is suggested by the authors to validate the significance of gender on social engineering susceptibility.

**Age.**

Age is another demographic explored by researchers that could potentially relate to social engineering susceptibility. One study determined that those in the age range of 28 – 38 were less likely to provide their own personal information when requested (Airehrour et al., 2018) while other studies determined that younger people were more likely to reveal a password when asked (Happ et al., 2016), were more susceptible to phishing attacks (Sheng et al., 2010), and were more susceptible to social engineering through the use of social networking websites (Algarni et al., 2015). Jagatic et al. (2007) studied the use of phishing emails that contained information found on recipients’ social networking sites. The phishing emails were sent to university students, and it was determined that freshmen were slightly more susceptible to opening the emails than were the seniors. Related to the discussion on gender, the study also determined that a phishing email sent by the opposite gender of the recipient had a greater chance of success than one sent by the same gender (Jagatic et al., 2007). Contributing to contradictory findings, Moody et al. (2017) determined that age was not a significant predictor of vulnerability in terms of phishing attacks. However, their research only included participants of a similar age in a single class at a university.

**Training.**

Training has been explored as it relates to social engineering susceptibility. Sheng et al. (2010) determined that the use of educational materials decreased the likelihood that individuals would provide information in response to a phishing email. Similarly, Airehrour et al. (2018) suggested that awareness training is a critical component of mitigating attacks, and Heartfield & Loukas (2015) proposed that training helps individuals identify cues in social engineering attempts. Several studies question the impact of social engineering training by claiming it is “too static and unresponsive to the changing cyber domain” (Williams et al., 2018, p.9) or that it is limited in its ability to affect people because knowledge imparted in the trainings is usually overshadowed by the impact of urgency cues in particular social engineering situations (Vishwanath et al., 2011).

**Cultural Identity.**

Cultural differences have been studied in the context of social engineering susceptibility. Bullee et al. (2015) studied Cialdini’s authority principle of persuasion (2007) and proposed that cultural differences in adherence to authority impact the strength in which it is used as an influencer. Butavicius et al. (2017) determined that the cultural focus on individual rather than group needs was a strong predictor in determining whether people can distinguish between safe and unsafe emails. Williams et al. (2018) studied phishing susceptibility and highlighted the importance of understanding differences between communication and email styles as a result of cultural variations.

**Other Variables.**

Other lesser studied variables researched as a means to predict social engineering susceptibility include length of employment and rank. Research has shown that newer employees could potentially be more susceptible to social engineering since they most likely do not know all of the employees or contacts they would be communicating with on the job and as a result, would be less likely to identify phishing emails (Williams et al., 2018). This finding is somewhat contradictory to another study that determined that when the sender of an email is known, the susceptibility to social engineering of the recipient increases (Moody et al., 2017). Newer employees would most likely not know the senders of emails they receive which would mean they are less susceptible in terms of falling victim to a phishing email.

Although studied infrequently, the rank of an employee can be used to help predict susceptibility to social engineering. Uebelacker & Quiel (2014) suggested that a manager, or someone with a higher rank, has greater access and ability to share important confidential information. However, they concluded that every individual has the potential to provide varying degrees and amounts of information to social engineers so rank is not that important.

To the best of the researcher’s knowledge, there have been no studies that explored other variables as predictors of social engineering susceptibility including education or hours worked, as well as studies that have been conducted in a small business setting. Most of the studies have been done in university settings with college students, staff, or faculty (Jansson & vonSolms, 2013; Vishwanath et al., 2011; Wright et al., 2010; Van Kleef et al., 2015; Snyman & Kruger, 2017; Zheng et al., 2018; Vishwanath et al., 2016; Moody et al., 2017).

**Small Business.**

Small businesses have the potential to be one of the most susceptible types of businesses to social engineering (Social-Engineer, 2018; Aguilar, 2015), and these attacks are increasing in occurrence (Harris, 2018). They often lack resources, both technical and human, to protect themselves from outside threats (Hiscox, 2018). These businesses usually understand the risks they face and take appropriate actions that align with their limited budgets. However, very rarely are they able to implement full-scale security safeguards to improve their resilience and reduce susceptibility (FSB, 2016) especially to business email compromise (BEC) schemes which are considered to be the most frequent type of attack for small businesses (Harris, 2018).

After a data breach or social engineering attack, a small business usually needs at minimum two days to return to normal business operations and often times it takes an entire week (FSB, 2016). This downtime for small businesses can have a substantial impact on their profits and viability to continue operations in the future (Hiscox, 2018). About half of small businesses that are victims of cyberattacks are forced to go out of business in the six months following the attack (LeClair, 2015).

Many small businesses also underestimate the amount of risk they face in terms of data breaches and social engineering attacks and become easily overwhelmed with trying to understand the significant risks they face on a daily basis (Social-Engineer, 2018). The limited number of staff is usually performing multiple roles in the company, and cybersecurity protections tend to rank lower on the list of priorities when compared to the other critical functions that must be completed in the course of business (FSB, 2016). It is for this reason that small businesses are appealing targets to attackers. These companies can be used as a gateway to obtain access to larger companies that likely have better security protections in place (Aguilar, 2015).

**Human Aspects of Information Security Questionnaire (HAIS-Q)**

The human aspects of information security questionnaire (HAIS-Q) was created by Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014) to study the relationship between knowledge, attitude, and behavior and information security policies. The questionnaire was originally developed as a result of a quantitative and qualitative study with over 200 employees from government organizations in Australia (Parsons et al., 2013). They attempted to measure information security awareness among employees and managers in these organizations. While employees scored at acceptable levels for knowledge, attitude, and behavior, the scores were higher specifically for the knowledge component. The researchers concluded that employees may have high knowledge regarding information security policies, but their behavior does not necessarily align with their level of knowledge. This conclusion was further supported by the qualitative interviews performed with members of management (Parsons et al., 2013).

This initial study served as the foundation for the development of the HAIS-Q in which the researchers created seven focus areas to measure knowledge, attitude, and behavior of employees when using a work computer. The questionnaire has been tested for validity and reliability (Parsons et al., 2014; Parsons et al., 2017). As of 2017, over 1,500 employees from a variety of industries in Australia have completed the HAIS-Q. Training and education programs in organizations can be tailored to specific employee needs based on the result of the HAIS-Q (Parsons, et al., 2017).

The HAIS-Q has been widely used in research studies. Butavicius, et al. (2017) used the questionnaire in conjunction with Cialdini’s (2007) principles of persuasion on business students from an Australian university. The researchers created online scenarios containing three types of emails including phishing, spear-phishing, and authentic, along with three of Cialdini’s (2007) principles, authority, social proof, and scarcity, as means of social engineering techniques. Participants in the study were asked to judge the safety of the various emails they were shown. At the end of the lab-based simulation, participants completed the HAIS-Q. Butavicius, et al. (2017) determined that culture and information security awareness were two of the strongest predictors in whether the participants were able to distinguish between safe and unsafe emails. Higher information security awareness was correlated with identification of malicious emails.

Pattinson et al. (2017) used the HAIS-Q in a study on bank employees in Australia and in another study with 500 employees from a variety of industries. The researchers concluded that information security awareness of the bank employees was about 20% higher than those in other industries. They studied the use of training in these organizations, and in a somewhat contrary finding to what they expected, the researchers determined that only 16% of the bank employees had experienced a formal education in information security compared to 27% of the generalized employee group from multiple industries.

The main focus of the HAIS-Q is to measure information security awareness, and several studies have found a link between awareness and susceptibility. Professionals in the information technology industry attribute social engineering success to the absence of information security awareness. Interviews with these industry professionals revealed to the researchers that people are simply unaware of issues in information security today, social engineering being one of them (Janczewski & Fu, 2010). Butavicius et al. (2017) concluded that information security awareness, as a self-report measure in the HAIS-Q, led to better detection and identification of suspicious emails.

To further support these findings, researchers have used interventions as a way to bring awareness of information security issues to individuals and then determine if there is a connection between these interventions and susceptibility to social engineering. Williams et al. (2018) used focus groups to measure the effectiveness of email banners as a means of brief communication with the participants. These banners urged viewers of emails to consider the safety and validity of the messages before clicking on any links. The banners brought an increased sense of awareness to people, making them more likely to distinguish between safe and unsafe emails, and therefore making them less susceptible to social engineering attacks via phishing emails.

Bullee et al. (2015) used three types of interventions, a leaflet, key chain, and poster, that contained reminders to employees about information security issues related to social engineering, sharing access, and password / PIN security, respectively. These interventions served as a method of awareness and significantly reduced the likelihood that employees would share their work keys when requested. Those employees who did not receive the intervention were almost three times more likely to comply with the request than those who experienced one of the three interventions (Bullee et al., 2015).

The HAIS-Q measures three components of an individual’s security awareness: knowledge, attitude, and behavior. A somewhat similar model based on the comparable foundational principles of the HAIS-Q is found in the suspicion, cognition, and automaticity model of phishing susceptibility (SCAM) as postulated by Vishwanath et al. (2016). This model was tested in two studies that involved phishing emails and suggested that cognitive ability of individuals can be piqued by suspicions about various types of cues. In addition, there are varying levels of automaticity, or routineness, in people’s actions especially as it relates to email behavior. The components of the model mentioned here can serve to detract from attempts to train individuals on social engineering susceptibility and therefore influence their knowledge, attitude, and behavior (Vishwanath et al., 2016).

Williams et al. (2018) acknowledged the importance of these previously mentioned cognitive capabilities in their study but suggested the application of standard, accepted practices and procedures to better understand susceptibility. One specific practice is that of organizational cognitive pressure which could lead to an increase in susceptibility to phishing emails. The larger point found in this research is that additional factors need to be considered when determining susceptibility. The researchers acknowledged their inability to collect demographic information from participants in their study (Williams et al., 2018) which could have added another layer to the data they collected from two different organizations regarding phishing susceptibility.

**Literature Review Conclusion**

The literature pertaining to social engineering susceptibility is rather broad in nature, spanning several different approaches and perspectives. Some of the limitations and deficiencies of other studies have been identified and used as the catalysts for this research. Many of the studies disregarded ethnic diversity of their populations (Pattinson et al., 2017; Happ et al., 2016; Goel et al., 2017; Moody et al., 2017; Heartfield, Loukas, & Gan, 2016) which is an important factor, especially considering the main point of social engineering is psychological manipulation to change behavior. Thought processes and behavioral actions can differ based on the culture in which individuals were raised, in which they work, and where they reside and can have major implications for understanding and perhaps even predicting employee behavior around information security in an organizational setting (Butavicius et al., 2017).

Vishwanath et al. (2011) concluded that susceptibility to social engineering is influenced by cognitive and information processing activities, but do they differ by demographics? Stewart & Jurjens (2016) experienced pushback during their research since many of the companies studied in the finance and technology industry are highly regulated by external entities. This particular study gathered data from a variety of industries to determine if this external regulation has an impact on employee susceptibility to social engineering based on data obtained from participants in each industry. Hasle, Kristiansen, Kintel, & Snekkenes (2005) created a social engineering resistance metric which can be linked to susceptibility explored in this research. High resistance achieved on their metric can be interpreted to mean low susceptibility to social engineering.

A report issued by the Computer Emergency Response Team (CERT) at Carnegie Melon (2014) notes a weak association between demographic characteristics and social engineering susceptibility and suggests future research on the subject to help clarify the existing literature. The prior studies that have been done using demographics have somewhat contradictory findings, further supporting the need for additional studies to be completed. Few, if any studies, have focused on the small business demographic who should not be excluded from consideration of susceptibility to social engineering (Social-Engineer, 2018). Studying social engineering in an organizational context, especially in the small business realm, can help companies better understand how their employees and their companies can be susceptible to the ever-increasing threat of social engineering.

**Chapter III**

**Methodology**

**Research Design**

The purpose of this research study was to determine if demographic features of employees in small business impact susceptibility to social engineering as measured on the Human Aspects of Information Security Questionnaire (HAIS-Q). A cross-sectional survey is the preferred technique of data collection since it provides an efficient and effective method to capture large amounts of data and perform analysis on the information collected (Fowler, 2009). It is important that the survey be cross-sectional, or collected at a single point in time, since internal and external factors could impact survey results. Internal factors can include the availability or pervasiveness of employee training and external factors can include widely publicized data breaches or trending economic / social issues, all of which could impact employee responses to survey questions.

The survey collected data using the REDcap online platform which allowed employees to complete the survey on a computer or mobile device. Online data collection provides a cost-effective process that makes it easy and convenient for the survey participants to respond to the questions and also an efficient process for the researcher to collect and analyze large amounts of data.

**Sample**

The population in this study included employees from small businesses, defined here as having less than 25 employees, from a variety of industries in northeastern Pennsylvania. Sampling design for this population is a single stage, nonprobability, non-stratified sample. A nonprobability sampling method is used for most opinion, political, and marketing polling (Fowler, 2009) and is therefore appropriate for this study. These small business employees are a convenience sample, located in the same geographic region and easily accessible to the researcher.

The concept of nonresponse is a consideration for the researcher. In this study, the researcher and the associated university may not have been recognizable to the participants so understanding predicted response rates was challenging. Also, the researcher is utilizing an online survey but was unaware of how often the employees use the internet even though they have a company email address (Fowler, 2009). Nonresponse by employees was attempted to be addressed by understanding the possible reasons for it. One of those reasons may be employee time away from work for travel or personal time off. The electronic survey was open for several weeks which reduces the chance for scheduling conflicts and work load fluctuations that could have impacted an employee’s ability to complete the survey.

Participants were included in the study based on the following criteria. They must be 18 years of age, employed by a small business in northeastern Pennsylvania, and must have a company issued email address along with access to a computer or mobile device. Since the survey was sent and completed electronically, those without company email addresses were excluded from the survey. Participants were recruited based on direct communication with the owners and employees of small businesses (See Appendix A). It was clear that there were no ramifications for not participating in the study and job status, position, and rank in the company would not be affected.

Active informed consent was obtained before participants began the survey. The informed consent form provided information about the purpose of the study, what the participants would be asked to do, the risks and benefits of the study, the opportunity for payment or reward for participating, information about confidentiality of respondents and the results, and the contact information of the researcher and dissertation chair (See Appendix B). The survey would not begin until an employee read the document and provided an electronic signature.

**Instrumentation**

**HAIS-Q.**

The Human Aspects of Information Security Questionnaire (HAIS-Q) was originally designed by Parsons et al. (2014) to measure information security awareness based on the components of knowledge, attitude, and behavior of individuals. They specifically identified focus areas to measure the various components including password management, email use, internet use, social networking site use, incident reporting, mobile computing, and information handling. This survey was designed based on their qualitative research with senior management in Australian government entities who reported that being unaware and naïve would lead to more data breaches than actual malicious intent (Parsons et al., 2014).

The HAIS-Q has been tested for validity and reliability using a variety of mechanisms. Prior to utilizing this questionnaire, a survey design expert reviewed and completed the study and provided feedback to the researchers. Next, the researchers utilized cognitive testing with an information security expert who voiced concerns and questions while completing the survey. Finally, they conducted a pilot study with 120 employees working in Australia. The results showed that all three constructs, including knowledge, attitude, and behavior, had a Cronbach’s alpha coefficient above the benchmark of 0.70. Ten statements in the survey were changed slightly after an analysis of Pearson correlations determined that the wording was too complex. After going through these three tests of validity and reliability, the researchers utilized this survey in their larger study of over 1,000 employees in Australia (Parsons, et al., 2014).

Parsons, et al. (2017) continued their research using the HAIS-Q in a variety of industries including education, government, and financial, reaching over 1,600 participants. They performed factor analysis and determined correlation coefficients ranging from .51 and .78 indicating a strong association between the 21 areas of interest contained within the seven focus areas. The researchers determined a Kaiser-Myer-Olkin value of 0.96 and also determined statistical significance using Barlett’s Test of Sphericity (x2(210) = 5824.52, p < .001). All of these findings promote construct validity of this survey which supports the use of it in this particular study on social engineering susceptibility.

The use of this survey for a purpose outside of its intended use is a limitation in this research study. The HAIS-Q specifically measures information security awareness in terms of knowledge, attitude, and behavior. However, many other research studies have identified a link between information security awareness and susceptibility to social engineering. These findings support the use of the HAIS-Q in this study aimed at determining the relationship, if any, between employee demographics and social engineering susceptibility. For example, security awareness among employees leads to the protection of confidential information (Stewart & Jurjens, 2016) and monitoring that awareness (Pyzik, 2015) or implementing awareness training (Janczewski & Fu, 2010) can help decrease the success of a social engineering attack. Additionally, Janzewski & Fu (2010) determined that employees should be educated on social engineering which increases their awareness and in turn causes them to be resistant to social engineering. Low susceptibility to social engineering translates to a high resistance to social engineering, and several researchers have even developed a social engineering resistance (SER) metric to help implement countermeasures to mitigate social engineering attacks (Hasle et al., 2005).

A modified version of the HAIS-Q was used in this research study. All focus areas identified previously were used in the study except for *social media use* and *incident reporting*. *Social media use* was excluded because the statements mostly related to knowledge, attitude, and behavior exhibited outside of the workplace. *Incident reporting* was excluded because the statements involved reactions on behalf of the participants as a result of of others’ knowledge, attitude, and behavior rather than their own. Employees were prompted to read a statement related to their knowledge, attitude, or behavior about the focus areas of password management, email use, internet use, mobile devices, and information handling. Question #38 has been modified slightly. The original text, “Disposing of sensitive print-outs by putting them in the *rubbish* bin is safe” has been changed to “Disposing of sensitive print-outs by putting them in the *trash* bin is safe.” The intention of this change was to use a synonym that would be understandable to the population taking this survey. Although it is possible that changing this one word could have an impact on the reliability and validity of the survey instrument, the researcher deemed the likelihood of such an impact as unlikely and determined that the change was necessary to avoid confusion by the participants.

Participants provided answers using a 5-point Likert scale originally developed by Rensis Likert as a way to measure attitudes of respondents along a continuum. It tends to provide a more robust measurement than yes or no answers (Likert, 1932). The possible answer choices included *Strongly Agree, Agree, Neither Agree Nor Disagree, Disagree, and Strongly Disagree.* To align with the original researchers’ delivery of the HAIS-Q, the questions within each grouping of knowledge, attitude, and behavior were provided to each participant in sequential order. The list of questions is provided in Appendix C.

The statements from the HAIS-Q are both positively and negatively framed to diminish the risk of an employee looking for a pattern in answers. The following questions are reverse scored: #1, 2, 4, 6, 7, 9, 11, 13, 15, 16, 18, 19, 20, 24, 25, 28, 29, 32, 35, 37, 38, 40, 41, and 45. However, as with any survey mechanism there exists the possibility of social desirability bias where respondents may answer questions in a socially desirable way to make themselves appear more likeable, more intelligent, or having provided the “correct” answer (Social Desirability Bias, 2004).

Each statement in the HAIS-Q has point values assigned to the answers based on the Likert scale. For positively framed statements, *Strongly Agree* was worth 5 points, *Agree* was worth 4 points, *Neutral* was worth 3 points, *Disagree* was worth 2 points, and *Strongly Disagree* was worth 1 point. Negatively framed statements were scored as follows: *Strongly Agree* was worth 1 point, *Agree* was worth 2 points, *Neutral* was worth 3 points, *Disagree* was worth 4 points, and *Strongly Disagree* was worth 5 points. Each participant’s survey resulted in an overall score which totaled the points assigned from each statement answer. The modified HAIS-Q used in this survey contained 45 statements meaning that the highest possible total score was 225 and the lowest possible score was 45 assuming all questions were answered. This survey was intended to measure information security awareness so the higher the score, the higher the employee’s awareness. If an employee has high information security awareness, then the employee will be ranked low on susceptibility to social engineering. Conversely, if an employee has low information security awareness, then the employee will be ranked high on susceptibility to social engineering.

**High Susceptibility** **Low Susceptibility**

**Low Awareness**  **High Awareness**

45 90 135 180 225

*Figure 4.* ModifiedHAIS-Q scoring. This figure provides the range of possible scores on the modified version of the HAIS-Q, ranking respondents from low to high susceptibility to social engineering.

**Demographic Data Collection.**

The second data collection instrument used in this survey asked respondents to answer questions related to their demographics and current work situation (See Appendix D). Participants were asked to provide their gender by choosing *male*, *female*, *other*, or *prefer not to* *answer* and the numerical value for their age as a whole number. They were asked for their highest level of education completed which can range from *less than a high school diploma* through a *terminal degree*. Survey respondents were asked to provide the length of employment with their current company and were given five choices that range from *less than one year* to *more than ten years*. The next question asked the average number of hours per week that the employee works rounded to the nearest whole number and what industry the company operates in. Industry options provided include *healthcare*, *marketing*, *construction*, *technology*, *nonprofit*, *law*, *finance*, *insurance*, and *other* if none of the options fit the employee’s current industry.

Participants were asked how many times per year on average they received training on cybersecurity awareness. Five options were provided that ranged from zero to more than three times. Since the original intent of the HAIS-Q is to measure awareness, this question in the instrument aligns closely with the overall purpose of the HAIS-Q. Employees were then asked to designate their rank in the company as either *owner / highest ranking official* or *non-owner / non-highest ranking official*. The last question in this survey instrument asked the employees to choose the option that most closely resembles their cultural identity. The choices were *American*, *Latino*, *Asian*, *Indian, Canadian*, *British/European, Middle Eastern, African,* and *other* if none of the options aligned with the employee’s cultural background.

**Procedures**

The researcher requested an exempt review from the Exempt Review Committee of the Institutional Review Board at Marywood University. This study posed no greater than minimal risk of everyday activities. Survey data collection commenced once approval was received.

An invitation to participate in this survey was emailed to the potential participants’ company email addresses directly from the researcher. The email contained the recruitment letter which explained the purpose of the study and the expectations of being a participant. The link to the survey was also posted to the researcher’s Facebook and LinkedIn pages as a way to recruit participants. Individuals must have met the criteria which included being at least 18 years of age, a full-time or part-time employee of a small business in northeastern Pennsylvania, and having a company email address. If they qualified and chose to participate in the survey, they were directed to complete an informed consent form which again provided information about the purpose of the study, what the participants will be asked to do, the risks and benefits of the study, the opportunity for payment or reward for participating, information about confidentiality of respondents and the results, and the contact information of the researcher and dissertation chair. The survey did not begin until an employee read the informed consent document and provided an electronic signature.

Participants could have completed the survey on any computer or device that allowed them to access it. This could have included a personal work computer, a shared work computer, a personal home computer, or a mobile device. After the initial email was sent to recruit participants, a follow-up email was sent two weeks later as a reminder to complete the survey in an attempt to gain additional data. A third and final email was sent two weeks after the second reminder. The survey was open to participants for a total of eight weeks.

The participants were required to self-report on statements related to knowledge, attitude, and behavior of information security using a 5-point Likert scale. Instructions were provided in the survey. In addition, participants were asked to provide various demographic information about themselves including gender, age, education, length of employment with a company, hours worked, industry, training, rank, and cultural identity.

Only the main researcher and her three dissertation committee members had access to the data records. The interpreted data has the potential to be shared with other agencies and institutions, but this did not impact the confidentiality of the survey responses. Information used in any written or presented report will not make it possible to identify respondents. Records will be kept for six months and destroyed immediately after that time period has elapsed.

**Analysis of Data**

The researcher utilized IBM SPSS Version 26 to analyze the results of the research study. General descriptive statistics including mean and standard deviation were calculated on the dataset to describe the information collected from the chosen sample to address subproblems 1 – 9 listed previously. Multiple regression was used to address the last subproblem, How do demographic characteristics of the participants predict social engineering susceptibility?

A statistically significant difference was determined if *p* < 0.05.

**Supplemental Analysis**

The HAIS-Q utilized in this study examined the knowledge, attitude, and behavior of the participants and provided a total susceptibility score for them. The relationship among these four variables was measured with the use of a Pearson Correlation Coefficient. Additional supplemental analysis of three more regressions was run on the dataset to determine if a significant model exists to predict knowledge, attitude, and behavior from the demographic variables. Knowledge, attitude, and behavior scores were also analyzed to determine if any of them are predictors of each other.

Additional supplemental analysis was done by dividing the data into groups based on some of the demographic factors:

Gender by knowledge, attitude, behavior, and social engineering susceptibility was analyzed using four independent sample t tests.

Age by knowledge, attitude, behavior, and social engineering susceptibility was analyzed using four Pearson correlations.

Length of employment by knowledge, attitude, behavior, and social engineering susceptibility was analyzed using four ANOVAs.

Education by knowledge, attitude, behavior, and social engineering susceptibility was analyzed using four ANOVAs.

Hours worked by knowledge, attitude, behavior, and social engineering susceptibility was analyzed using four Pearson correlations.

Industry by knowledge, attitude, behavior, and social engineering susceptibility was analyzed using four independent sample t tests.

Training by knowledge, attitude, behavior, and social engineering susceptibility was analyzed using four ANOVAs.

Rank by knowledge, attitude, behavior, and social engineering susceptibility was analyzed using four independent sample t tests.

Cultural identity by knowledge, attitude, behavior, and social engineering susceptibility was analyzed using four independent sample t tests.

**Chapter IV**

**Results**

The data set consists of 95 participant responses collected over an eight-week period. Two additional participants attempted to complete the study but did not meet the requirements for inclusion. All questions from all participants were answered. Case # 52 had one adjustment made regarding the response for *number of hours worked*. The response of 285 hours was removed since this would be an impossible number of hours to work in one week.

Respondents to this survey included owners and employees of small businesses in northeastern Pennsylvania, defined here as those with less than 25 employees, who also have a company email address and are at least 18 years of age.

The Kolmogorov-Smirnov test of normality shows that the data is normally distributed because all four variables had *p* values greater than 0.05. (ISA Score, *p* = .20; Knowledge Score, *p* = .20; Attitude Score, *p* = .09; Behavior Score, *p* = .20)

Descriptive statistics were computed on the data set. The frequency distributions of the variables are shown below and address subproblems 1 – 9.

**Subproblems 1 – 9**

Table 1 depicts a frequency distribution of gender including male, female, other, and prefer not to answer. Note that slightly more than half of the participants were male (*n* = 54).

Table 1

*Participant Gender (n = 95)*

|  |  |  |
| --- | --- | --- |
| Gender | Frequency | Percent |
| Male | 54 | 56.8 |
| Female | 38 | 40.0 |
| Prefer Not to Answer | 3 | 3.2 |

The mean age of participants was 42.6 years old (sd +/- 12.5), while the median was 41 (19 – 75). See Appendix E for the frequency distribution of age.

Table 2 depicts a frequency distribution of highest level of education ranging from less than a high school diploma to a terminal degree. Most participants had a maximum of a bachelor’s degree while none had less than a high school diploma.

Table 2

*Participant Education (n = 95)*

|  |  |  |
| --- | --- | --- |
| Education | Frequency | Percent |
| High School Diploma | 10 | 10.5 |
| Associate’s Degree | 12 | 12.6 |
| Bachelor’s Degree | 41 | 43.2 |
| Master’s Degree | 25 | 26.3 |
| Terminal Degree | 7 | 7.4 |

Because regression was used, the education variable was recoded into two dummy variables using high school diploma as the reference category, first with a comparison to participants who completed an associate’s or bachelor’s degree, and then with a comparison to participants who completed a master’s or terminal degree.

Table 3 shows a frequency distribution of length of employment with the company. Note that most participants have worked at their current company for less than 10 years (*n* = 56).

Table 3

*Participant Length of Employment (n = 95)*

|  |  |  |
| --- | --- | --- |
| Length of Employment | Frequency | Percent |
| Less than 1 Year | 10 | 10.5 |
| 1 – 3 Years | 14 | 14.7 |
| 4 – 6 Years | 20 | 21.1 |
| 7 – 9 Years | 12 | 12.6 |
| 10 or more Years | 39 | 41.1 |

Because regression was used, this variable was recoded into a dichotomous variable as shown below.

Table 3.1

*Participant Length of Employment Recoded (n = 95)*

|  |  |  |
| --- | --- | --- |
| Length of Employment | Frequency | Percent |
| Less than 10 Years | 56 | 58.9 |
| 10 or More Years | 39 | 41.1 |

Table 4 depicts a frequency distribution for how many times on average per year the employee or owner has received cybersecurity awareness training. Most of the participants have received cybersecurity awareness training (*n* = 56) at least once on average per year over the past three years.

Table 4

*Average Times Per Year Training Received (n = 95)*

|  |  |  |
| --- | --- | --- |
| Training Received Per Year | Frequency | Percent |
| 0 | 39 | 41.1 |
| 1 time | 30 | 31.6 |
| 2 times | 6 | 6.3 |
| 3 times | 7 | 7.4 |
| More than 3 times | 13 | 13.7 |

Because regression was used, the training variable has been recoded into a dichotomous variable as shown below.

Table 4.1

*Employee Training Received Recoded (n = 95)*

|  |  |  |
| --- | --- | --- |
| Training Received | Frequency | Percent |
| No | 39 | 41.1 |
| Yes | 56 | 58.9 |

Table 5 depicts a frequency distribution of industry in which the employee or owner works. Most participants identified with the industry of *other* (*n* = 37) with technology being the second highest industry (*n* = 27).

Table 5

*Participant Industry (n = 95)*

|  |  |  |
| --- | --- | --- |
| Industry | Frequency | Percent |
| Healthcare | 4 | 4.2 |
| Marketing | 3 | 3.2 |
| Construction | 4 | 4.2 |
| Technology | 27 | 28.4 |
| Nonprofit | 11 | 11.6 |
| Law | 3 | 3.2 |
| Finance | 5 | 5.3 |
| Insurance | 1 | 1.1 |
| Other | 37 | 38.9 |

Because regression was used, the industry variable has been recoded into a dichotomous variable as shown below.

Table 5.1

*Participant Industry Recoded (n = 95)*

|  |  |  |
| --- | --- | --- |
|  | Frequency | Percent |
| Non-Technology | 68 | 71.6 |
| Technology | 27 | 28.4 |

Table 6 shows a frequency distribution of rank in the company which includes owner / highest ranking official or non-owner / non-highest ranking official. Note that most participants were an owner / highest ranking official (*n* = 61).

Table 6

*Participant Rank (n = 95)*

|  |  |  |
| --- | --- | --- |
| Rank | Frequency | Percent |
| Owner / Highest Ranking Official | 61 | 64.2 |
| Non-Owner / Highest Ranking Official | 34 | 35.8 |

Table 7 depicts a frequency distribution of cultural identity. Over 93% of participants (*n* = 89) identified as American.

Table 7

*Cultural Identity (n = 95)*

|  |  |  |
| --- | --- | --- |
| Cultural Identity | Frequency | Percent |
| American | 89 | 93.7 |
| Latino | 1 | 1.1 |
| Asian | 1 | 1.1 |
| Indian | 1 | 1.1  Middle |
| Middle Eastern | 1 | 1.1 |
| Other | 2 | 2.1 |

Because regression was utilized to analyze cultural identity, this variable was recoded into dichotomous variables. See table below.

Table 7.1

*Recode of Cultural Identity (n = 95)*

|  |  |  |
| --- | --- | --- |
| Cultural Identity | Frequency | Percent |
| American | 89 | 93.7 |
| Non-American | 6 | 6.3 |

**Subproblem 10**

**HAIS-Q.**

The HAIS-Q consists of three sections concerning the respondents’ knowledge, attitude, and behavior. These sections were included in the total information security awareness score but were also calculated separately for each participant. See the supplemental analysis section for the summation of participant responses to each question.

The mean knowledge score is 58.6 (sd +/- 9.4), while the median is 58 (35 – 75). The mean attitude score is 65 (sd +/- 7.3), while the median is 65 (39 - 75). The mean behavior score is 62.3 (sd +/- 7.6), while the median is 63 (36 - 75). See Appendix F for the frequencies of knowledge, attitude, and behavior scores.

The total of the respondents’ knowledge, attitude, and behavior scores were combined to determine an information security awareness (ISA) score. The mean ISA score is 185.9 (sd +/- 21.92), while the median is 186 (118 – 225). See Appendix G for the frequencies of the ISA scores.

The ISA score was then converted to an employee susceptibility score with the understanding that the higher the ISA, the lower the susceptibility (Janczewski & Fu, 2010; Parsons et al., 2014; Pyzik, 2015). The ISA scale includes a possible score range from 45 – 225. This scale was converted to an inverse susceptibility scale ranging from 0 – 100. The following formula was used for the conversion: ((ISA Score – 225) \* (100/180) \* - 1). See Appendix G for a frequency distribution of the susceptibility scores. The mean susceptibility score is 21.71 (sd +/- 12.18), while the median is 21.67 (0 – 59.44).

**Multiple Regression.**

Scale level variables including the independent variables, age and weekly hours worked, and the dependent variable, susceptibility score, were examined for outliers. Any outliers were checked by analyzing z-scores, and none of the outliers showed z-scores +/- 3.29. Multivariate outliers were examined using Mahalanobis distance. The minimum (4.45) and the maximum (25.58) were below the critical cutoff of 29.59. Cook’s distance was found to be 0.207, well below a value of 1. None of the coefficient correlations exceeded a value of 0.3 and the variance inflation factor was below 10, both of which do not suggest any issues with multicollinearity.

A multiple linear regression was calculated predicting participants’ susceptibility score based on their gender, age, education, length of employment, average number of hours worked per week, industry, training, rank, and cultural identity. The regression equation was not significant (F(10, 80) = .583, *p* > .05) with an R2 of .068. None of the independent variables are significant predictors of susceptibility score. Thus the null hypothesis, demographic characteristics of employees in small business do not predict susceptibility to social engineering,

was not rejected.

The regression equation model is as follows:

Y = a + b *Age* + c *DGender* + d *DUG* + e *DGrad* + f *DEmp* + g *DTraining* + h *DHours* + i *DCulture* + j *DInd*+ k *DRank* + ∈

*Age* = natural number for age of participant

*DGender* = Gender, where 0 = male and 1 = female

*DUG*= Education Dummy Variable, where 0 = high school diploma, Master’s Degree, and Terminal Degree and 1 = Associate’s Degree and Bachelor’s Degree

*DGrad* = Education Dummy Variable, where 0 = high school diploma, Associate’s Degree, and Bachelor’s Degree and 1 = Master’s Degree and Terminal Degree

*DEmp* = Length of Employment, where 0 = less than 10 years and 1 = more than 10 years

*DTraining* = Training on average per year where 0 = no training and 1 = training

*DHours* = natural number for the Weekly Hours Worked

*DCulture* = Cultural Identity, where 0 = American and 1 = Non-American

*DInd* = Industry, where 0 = Non-Technology and 1 = Technology

*DRank* = Rank, where 0 = Non-Owner and 1 = Owner

∈ = residual error

Table 8

*Multivariate Regression Results*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Coefficient | Std. Error | Beta | *t* | *p* |
| a (y-intercept) | 37.63 | 11.34 | - | 3.32 | < .05 |
| b (Age) | -0.10 | 0.13 | -.10 | -0.73 | .46 |
| c (Gender) | -1.18 | 3.14 | -.05 | -0.38 | .71 |
| d (Associate / Bachelor) | -5.86 | 4.41 | -.24 | -1.33 | .19 |
| e (Master / Terminal) | -6.07 | 4.66 | -.24 | -1.30 | .20 |
| f (Employment Length) | 3.67 | 3.25 | .15 | 1.13 | .26 |
| g (Training) | -1.83 | 2.82 | -.08 | -0.65 | .52 |
| h (Weekly Hours) | -0.10 | 0.10 | -.11 | -0.94 | .35 |
| i (Cultural Identity) | -0.85 | 5.42 | -.02 | -0.16 | .88 |
| j (Industry) | 0.47 | 3.34 | .02 | 0.14 | .89 |
| k (Rank) | -1.46 | 3.04 | -.06 | -.48 | .63 |

**Supplemental Analysis**

**Respondent Answers.**

The table below shows participant responses to the knowledge, attitude, and behavior questions of the HAIS-Q. Note that the top three knowledge questions that participants disagreed or strongly disagreed with are: *It is acceptable to use my social media passwords on my work accounts; Sensitive print-outs can be disposed of in the same way as non-sensitive ones;* and *I am allowed to leave print-outs containing sensitive information on my desk overnight.* The top three attitude questions that participants disagreed or strongly disagreed with are: *Nothing bad can happen if I click on a link in an email from an unknown sender; When working in a café, it’s safe to leave my laptop unattended for a minute;* and *It’s risky to leave print-outs that contain sensitive information on my desk overnight.* The top three behavior questions that participants disagreed or strongly disagreed with are: *If an email from an unknown sender looks interesting, I click on a link within it; When working in a public space, I leave my laptop unattended;* and *I send sensitive work files using a public wi-fi network.*

Participants agreed or strongly agreed with the following three knowledge questions more than any others: *A mixture of letters, numbers, and symbols is necessary for work passwords; While I am at work, I shouldn’t access certain websites;* and *If I find a USB stick in a public place, I shouldn’t plug it into my work computer.* Participants agreed or strongly agreed with the following three attitude questions more than any others: *It’s risky to open an email attachment from an unknown sender; Just because I can access a website at work, doesn’t mean that it’s safe;* and *It’s risky to send sensitive work files using a public wi-fi network*. Participants agreed or strongly agreed with the following 3 behavior questions more than any others: *I use a combination of letters, numbers, and symbols in my work passwords; When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed;* and *I wouldn’t plug a USB stick found in a public place into my work computer.*

Table 9

*HAIS-Q Responses*

|  | Strongly Disagree | Disagree | Neither Agree nor Disagree | Agree | Strongly Agree |
| --- | --- | --- | --- | --- | --- |
| **Knowledge** |  |  |  |  |  |
| It is acceptable to use my social media passwords on my work accounts. | 47 (49%) | 25 (26%) | 9 (9%) | 13 (14%) | 1 (1%) |
| I am allowed to share my work passwords with colleagues. | 41 (43%) | 25 (26%) | 14 (15%) | 11 (12%) | 4 (4%) |
| A mixture of letters, numbers, and symbols is necessary for work passwords. | 6 (6%) | 5 (5%) | 1 (1%) | 40 (42%) | 43 (45%) |
| I am allowed to click on any links in emails from people I know. | 24 (25%) | 17 (18%) | 17 (18%) | 34 (36%) | 3 (3%) |
| I am not permitted to click on a link in an email from an unknown sender. | 8 (8%) | 10 (10%) | 12 (13%) | 28 (29%) | 37 (39%) |
| I am allowed to open email attachments from unknown senders. | 45 (47%) | 19 (20%) | 10 (10%) | 14 (15%) | 7 (7%) |
| I am allowed to download any files onto my work computer if they help me to do my job. | 29 (30%) | 18 (19%) | 9 (9%) | 28 (29%) | 11 (12%) |
| While I am at work, I shouldn’t access certain websites. | 4 (4%) | 2 (2%) | 5 (5%) | 32 (34%) | 52 (55%) |
| I am allowed to enter any information on any website if it helps me do my job. | 28 (29%) | 27 (28%) | 15 (16%) | 18 (19%) | 7 (7%) |
| When working in a public place, I have to keep my laptop with me at all times. | 6 (6%) | 8 (8%) | 12 (13%) | 29 (30%) | 40 (42%) |
| I am allowed to send sensitive work files via a public wi-fi network. | 42 (44%) | 20 (21%) | 20 (21%) | 11 (12%) | 2 (2%) |
| When working on a sensitive document, I must ensure that strangers can’t see my laptop screen. | 1 (1%) | 13 (14%) | 7 (7%) | 37 (39%) | 37 (39%) |
| Sensitive print-outs can be disposed of in the same way as non-sensitive ones. | 55 (58%) | 25 (26%) | 3 (3%) | 7 (7%) | 5 (5%) |
| If I find a USB stick in a public place, I shouldn’t plug it into my work computer. | 7 (7%) | 0 (0%) | 6 (6%) | 19 (20%) | 63 (66%) |
| I am allowed to leave print-outs containing sensitive information on my desk overnight. | 42 (44%) | 27 (28%) | 8 (8%) | 10 (10%) | 8 (8%) |
| **Attitude** |  |  |  |  |  |
| It is safe to use the same passwords for social media and work accounts. | 48 (50%) | 30 (32%) | 9 (9%) | 8 (8%) | 0 (0%) |
| It’s a bad idea to share my work passwords, even if a colleague asks for it. | 2 (2%) | 7 (7%) | 10 (10%) | 42 (44%) | 34 (36%) |
| It’s safe to have a work password with just letters. | 44 (46%) | 43 (45%) | 5 (5%) | 3 (3%) | 0 (0%) |
| It’s always safe to click on links in emails from people I know. | 34 (36%) | 40 (42%) | 11 (12%) | 9 (9%) | 1 (1%) |
| Nothing bad can happen if I click on a link in an email from an unknown sender. | 78 (82%) | 16 (17%) | 0 (0%) | 1 (1%) | 0 (0%) |
| It’s risky to open an email attachment from an unknown sender. | 1 (1%) | 1 (1%) | 2 (2%) | 29 (30%) | 62 (65%) |
| It can be risky to download files on my work computer. | 1 (1%) | 3 (3%) | 7 (7%) | 40 (42%) | 44 (46%) |
| Just because I can access a website at work, doesn’t mean that it’s safe. | 1 (1%) | 0 (0%) | 0 (0%) | 45 (47%) | 49 (52%) |
| If it helps me to do my job, it doesn’t matter what information I put on a website. | 40 (42%) | 40 (42%) | 5 (5%) | 10 (10%) | 0 (0%) |
| When working in a café, it’s safe to leave my laptop unattended for a minute. | 59 (62%) | 30 (32%) | 4 (4%) | 1 (1%) | 1 (1%) |
| It’s risky to send sensitive work files using a public wi-fi network. | 5 (5%) | 1 (1%) | 3 (3%) | 42 (44%) | 44 (46%) |
| Disposing of sensitive print-outs by putting them in trash bins is safe. | 3 (3%) | 2 (2%) | 7 (7%) | 42 (44%) | 41 (43%) |
| If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer. | 58 (61%) | 26 (27%) | 6 (6%) | 2 (2%) | 3 (3%) |
| It’s risky to leave print-outs that contain sensitive information on my desk overnight. | 74 (78%) | 15 (16%) | 2 (2%) | 2 (2%) | 2 (2%) |
| **Behavior** |  |  |  |  |  |
| I use different passwords for social media and work accounts. | 2 (2%) | 9 (9%) | 6 (6%) | 32 (34%) | 46 (48%) |
| I share my work passwords with colleagues. | 37 (39%) | 30 (32%) | 10 (10%) | 16 (17%) | 2 (2%) |
| I use a combination of letters, numbers, and symbols in my work passwords. | 3 (3%) | 2 (2%) | 1 (1%) | 35 (37%) | 54 (57%) |
| I don’t always click on links in emails just because they come from someone I know. | 3 (3%) | 6 (6%) | 4 (4%) | 49 (52%) | 33 (35%) |
| If an email from an unknown sender looks interesting, I click on a link within it. | 62 (65%) | 23 (24%) | 7 (7%) | 1 (1%) | 2 (2%) |
| I don’t open email attachments if a sender is unknown to me. | 7 (7%) | 2 (2%) | 11 (12%) | 22 (23%) | 53 (56%) |
| I download any files onto my work computer that will help me get the job done. | 23 (24%) | 33 (35%) | 14 (15%) | 20 (21%) | 5 (5%) |
| When accessing the internet at work, I visit any website that I want to. | 29 (30%) | 34 (36%) | 13 (14%) | 15 (16%) | 4 (4%) |
| I assess the safety of websites before entering information. | 3 (3%) | 8 (8%) | 8 (8%) | 41 (43%) | 35 (37%) |
| When working in a public space, I leave my laptop unattended. | 62 (65%) | 26 (27%) | 6 (6%) | 1 (1%) | 0 (0%) |
| I send sensitive work files using a public wi-fi network. | 48 (50%) | 27 (28%) | 14 (15%) | 6 (6%) | 0 (0%) |
| I check that strangers can’t see my laptop screen if I’m working on a sensitive document. | 3 (3%) | 3 (3%) | 15 (16%) | 40 (42%) | 34 (36%) |
| When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed. | 5 (5%) | 0 (0%) | 6 (6%) | 29 (30%) | 55 (58%) |
| I wouldn’t plug a USB stick found in a public place into my work computer. | 2 (2%) | 1 (1%) | 3 (3%) | 18 (19%) | 71 (75%) |
| I leave print-outs that contain sensitive information on my desk when I’m not there. | 41 (43%) | 31 (33%) | 8 (8%) | 10 (10%) | 5 (5%) |

**Pearson Correlations – Knowledge, Attitude, and Behavior.**

A Pearson correlation coefficient was calculated for the relationship between participants’ knowledge, attitude, and behavior scores. A strong positive correlation was found between knowledge and attitude (*r* (93) = .698, *p* < .001), between knowledge and behavior (*r* (93) = .755, *p* < .001), and between attitude and behavior (*r* (93) = .713, *p* < .001) indicating a significant linear relationships between the two variables in each grouping respectively. As each participant’s category score increased, the scores in the other two categories increased.

The coefficient of determination was examined for knowledge, attitude, and behavior scores. 48.7% of the variation in attitude score and 57.0% of the variation in behavior score can be explained by the knowledge score. 48.7% of the variation in knowledge score and 50.8% of the variation in behavior score can be explained by the attitude score. 57% of the variation in knowledge score and 50.8% of the variation in attitude score can be explained by behavior score.

A strong negative correlation was found between knowledge and susceptibility (*r* (93) = -.921, *p* < 0.001), between attitude and susceptibility (*r* (93) = -.878, *p* < 0.001), and between behavior and susceptibility (*r* (93) = -.907, *p* < 0.001). As knowledge, attitude, and behavior scores increase, susceptibility to social engineering decreases.

The coefficient of determination was examined for susceptibility score. 84.8% of the variation in knowledge score, 77% of the variation in attitude score, and 82.2% of the variation in behavior score can be explained by susceptibility score.

**Demographics as Predictors of Knowledge, Attitude, and Behavior Scores.**

A series of multiple regression analyses was performed to examine the demographic predictors against the knowledge, attitude, and behavior scores. A multiple linear regression was calculated predicting participants’ knowledge score based on their gender, age, education, length of employment with a company, average number of hours worked per week, industry, training, rank, and cultural identity. The regression equation was not significant (F(10, 80) = .60, *p* > .05) with an R2 of .07. None of the independent variables are significant predictors of knowledge score.

Y = a + b *Age* + c *DGender* + d *DUG* + e *DGrad* + f *DEmp* + g *DTraining* + h *DHours* + i *DCulture* + j *DInd*+ k *DRank* + ∈

Y = Knowledge Score

*Age* = natural number for age of participant

*DGender* = Gender, where 0 = male and 1 = female

*DUG*= Education Dummy Variable, where 0 = high school diploma, Master’s Degree, and Terminal Degree and 1 = Associate’s Degree and Bachelor’s Degree

*DGrad* = Education Dummy Variable, where 0 = high school diploma, Associate’s Degree, and Bachelor’s Degree and 1 = Master’s Degree and Terminal Degree

*DEmp* = Length of Employment, where 0 = less than 10 years and 1 = more than 10 years

*DTraining* = Training on average per year where 0 = no training and 1 = training

*DHours* = natural number for the Weekly Hours Worked

*DCulture* = Cultural Identity, where 0 = American and 1 = Non-American

*DInd* = Industry, where 0 = Non-Technology and 1 = Technology

*DRank* = Rank, where 0 = Non-Owner and 1 = Owner

∈ = residual error

Table 10

*Multivariate Regression Results*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Coefficient | Std. Error | Beta | *t* | *p* |
| a (y-intercept) | 53.58 | 8.65 | - | 6.20 | < .001 |
| b (Age) | .08 | .10 | .11 | .84 | .40 |
| c (Gender) | .45 | 2.39 | .02 | .19 | .85 |
| d (Associate / Bachelor) | .91 | 3.36 | .05 | .27 | .79 |
| e (Master / Terminal) | 1.18 | 3.56 | .06 | .33 | .74 |
| f (Employment Length) | -4.32 | 2.48 | -.23 | -1.74 | .08 |
| g (Training) | 1.27 | 2.15 | .07 | .59 | .56 |
| h (Weekly Hours) | .05 | .08 | .08 | .69 | .49 |
| i (Cultural Identity) | -2.52 | 4.14 | -.07 | -.61 | .54 |
| j (Industry) | -.15 | 2.55 | -.01 | -.06 | .95 |
| k (Rank) | 1.99 | 2.32 | .11 | .86 | .39 |

A multiple linear regression was calculated predicting participants’ attitude score based on their gender, age, education, length of employment with a company, average number of hours worked per week, industry, training, rank, and cultural identity. The regression equation was not significant (F(10, 80) = .942, *p* > .05) with an R2 of .105. Even though the ANOVA showed no significance (*p* > 0.05), there was suggested significance in the two recoded education variables (*p* < 0.05). As education increased from a high school diploma to either an Associate’s / Bachelor’s degree or a Master’s / Terminal degree, attitude score increased. These findings need further exploration in future studies to determine if education does in fact predict attitude score.

Y = a + b *Age* + c *DGender* + d *DUG* + e *DGrad* + f *DEmp* + g *DTraining* + h *DHours* + i *DCulture* + j *DInd*+ k *DRank* + ∈

Y = Attitude Score

*Age* = natural number for age of participant

*DGender* = Gender, where 0 = male and 1 = female

*DUG*= Education Dummy Variable, where 0 = high school diploma, Master’s Degree, and Terminal Degree and 1 = Associate’s Degree and Bachelor’s Degree

*DGrad* – Education Dummy Variable, where 0 = high school diploma, Associate’s Degree, and Bachelor’s Degree and 1 = Master’s Degree and Terminal Degree

*DEmp* = Length of Employment, where 0 = less than 10 years and 1 = more than 10 years

*DTraining* = Training on average per year where 0 = no training and 1 = training

*DHours* = natural number for the Weekly Hours Worked

*DCulture* = Cultural Identity, where 0 = American and 1 = Non-American

*DInd* = Industry, where 0 = Non-Technology and 1 = Technology

*DRank* = Rank, where 0 = Non-Owner and 1 = Owner

∈ = residual error

Table 11

*Multivariate Regression Results*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Coefficient | Std. Error | Beta | *t* | *p* |
| a (y-intercept) | 55.09 | 6.74 | - | 8.17 | < .05 |
| b (Age) | -.01 | .08 | -.01 | -.06 | .95 |
| c (Gender) | -1.15 | 1.87 | -.08 | -.61 | .54 |
| d (Associate / Bachelor) | 6.65 | 2.62 | .46 | 2.53 | .01 |
| e (Master / Terminal) | 6.09 | 2.78 | .40 | 2.19 | .03 |
| f (Employment Length) | -.14 | 1.94 | -.01 | -.07 | .94 |
| g (Training) | .65 | 1.68 | .04 | .39 | .70 |
| h (Weekly Hours) | .04 | .06 | .08 | .69 | .49 |
| i (Cultural Identity) | 2.24 | 3.23 | .08 | .69 | .49 |
| j (Industry) | -.61 | 1.99 | -.04 | -.31 | .76 |
| k (Rank) | .39 | 1.81 | .03 | .22 | .83 |

A multiple linear regression was calculated predicting participants’ behavior score based on their gender, age, education, length of employment with a company, average number of hours worked per week, industry, training, rank, and cultural identity. The regression equation was not significant (F(10, 80) = .717, *p* > .05) with an R2 of .082. None of the independent variables are significant predictors of behavior score.

The regression equation is as follows:

Y = a + b *Age* + c *DGender* + d *DUG* + e *DGrad* + f *DEmp* + g *DTraining* + h *DHours* + i *DCulture* + j *DInd*+ k *DRank* + ∈

Y = Behavior Score

*Age* = natural number for age of participant

*DGender* = Gender, where 0 = male and 1 = female

*DUG*= Education Dummy Variable, where 0 = high school diploma, Master’s Degree, and Terminal Degree and 1 = Associate’s Degree and Bachelor’s Degree

*DGrad* = Education Dummy Variable, where 0 = high school diploma, Associate’s Degree, and Bachelor’s Degree and 1 = Master’s Degree and Terminal Degree

*DEmp* = Length of Employment, where 0 = less than 10 years and 1 = more than 10 years

*DTraining* = Training on average per year where 0 = no training and 1 = training

*DHours* = natural number for the Weekly Hours Worked

*DCulture* = Cultural Identity, where 0 = American and 1 = Non-American

*DInd* = Industry, where 0 = Non-Technology and 1 = Technology

*DRank* = Rank, where 0 = Non-Owner and 1 = Owner

∈ = residual error

Table 12

*Multivariate Regression Results*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Coefficient | Std. Error | Beta | *t* | *p* |
| a (y-intercept) | 48.60 | 7.12 | - | 6.83 | < .001 |
| b (Age) | .09 | .08 | .15 | 1.13 | .26 |
| c (Gender) | 2.81 | 1.97 | .18 | 1.43 | .16 |
| d (Associate / Bachelor) | 2.99 | 2.77 | .20 | 1.08 | .28 |
| e (Master / Terminal) | 3.66 | 2.93 | .23 | 1.25 | .22 |
| f (Employment Length) | -2.16 | 2.04 | -.14 | -1.06 | .30 |
| g (Training) | 1.37 | 1.77 | .09 | .78 | .44 |
| h (Weekly Hours) | .08 | .06 | .14 | 1.21 | .23 |
| i (Cultural Identity) | 1.82 | 3.41 | .06 | .54 | .59 |
| j (Industry) | -.08 | 2.10 | -.01 | -.04 | .97 |
| k (Rank) | .24 | 1.91 | .02 | .12 | .90 |

**Knowledge, Attitude, and Behavior Scores as Predictors.**

A simple linear regression was calculated to determine if the knowledge score predicts the attitude score. The regression equation was significant (F(1, 93) = 88.22, *p* < .001) with an R2 of .49. Participants’ predicted attitude score is equal to 33.28 + .541 (knowledge score). Participants average attitude score increased by .54 for each point increase in knowledge.

The regression equation is as follows:

Y = a + b *X*1 + ∈

Y = Attitude Score

*X*1  = Knowledge Score

∈ = residual error

Table 13

*Multivariate Regression Results*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Coefficient | Std. Error | Beta | *t* | *p* |
| a (y-intercept) | 33.28 | 3.42 | - | 9.74 | < .001 |
| b (Knowledge Score) | .541 | .06 | .70 | 9.39 | < .001 |

A simple linear regression was calculated to determine if the attitude score predicts the behavior score. The regression equation was significant (F(1, 93) = 96.28, *p* < .05) with an R2 of .51. Participants’ predicted behavior score is equal to 13.53 + .75 (attitude score). Participants average behavior score increased by .75 for each point increase in attitude.

The regression equation is as follows:

Y = a + b *X*1 + ∈

Y = Behavior Score

*X*1  = Attitude Score

∈ = residual error

Table 14

*Multivariate Regression Results*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Coefficient | Std. Error | Beta | *t* | *p* |
| a (y-intercept) | 13.53 | 5.00 | - | 2.70 | < .05 |
| b (Attitude Score) | .75 | .08 | .71 | 9.81 | < .05 |

A multiple linear regression was calculated to determine if knowledge and attitude scores predict the behavior score. The regression equation was significant (F(2, 92) = 81.07, *p* <.05) with an R2 of .64. Participants’ predicted behavior score is equal to 13.48 + .41 (knowledge score) + .38 (attitude score). Participants’ behavior score increased by .41 for each increase in knowledge score and by .38 for each increase in attitude score. The regression model is as follows:

Y = a + b *X*1 + c *X*2 + ∈

Y = Behavior Score

*X*1  = Knowledge Score

*X*2 = Attitude Score

∈ = residual error

Table 15

*Multivariate Regression Results*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Coefficient | Std. Error | Beta | *t* | *p* |
| a (y-intercept) | 13.48 | 4.32 | - | 3.12 | < .05 |
| b (Knowledge Score) | .41 | .07 | .50 | 5.73 | < .05 |
| c (Attitude Score) | .38 | .09 | .36 | 4.14 | < .05 |

**Gender.**

An independent sample t test was calculated comparing the mean knowledge score of participants who identified as male to the mean knowledge score of participants who identified as female. No significant difference was found (*t*(90) = .24, *p* > .05). The mean knowledge score of males (*M* = 58.44, *sd* = 9.50) was not significantly different from the mean knowledge score of females (*M* = 57.97, *sd* = 8.89).

An independent sample t test was calculated comparing the mean attitude score of participants who identified as male to the mean attitude score of participants who identified as female. No significant difference was found (*t*(90) = .73, *p* > .05). The mean attitude score of males (*M* = 65.26, *sd* = 7.34) was not significantly different from the mean attitude score of females (*M* = 64.13, *sd* = 7.14).

An independent sample t test was calculated comparing the mean behavior score of participants who identified as male to the mean behavior score of participants who identified as female. No significant difference was found (*t*(90) = -1.26, *p* > .05). The mean behavior score of males (*M* = 61.20, *sd* = 7.94) was not significantly different from the mean behavior score of females (*M* = 63.21, *sd* = 6.94).

An independent sample t test was calculated comparing the mean susceptibility score of participants who identified as male to the mean susceptibility score of participants who identified as female. No significant difference was found (*t*(90) = .09, *p* > .05). The mean susceptibility score of males (*M* = 22.27, *sd* = 12.25) was not significantly different from the mean susceptibility score of females (*M* = 22.05, *sd* = 11.77).

**Age.**

A Pearson correlation was calculated examining the relationship between participants’ knowledge score and age. A weak correlation that was not significant was found (*r* (91) = .000, *p* > .05). Knowledge score is not related to age.

A Pearson correlation was calculated examining the relationship between participants’ attitude score and age. A weak correlation that was not significant was found (*r* (91) = -.06, *p* > .05). Attitude score is not related to age.

A Pearson correlation was calculated examining the relationship between participants’ behavior score and age. A weak correlation that was not significant was found (*r* (91) = .002, *p* > .05). Behavior score is not related to age.

A Pearson correlation was calculated examining the relationship between participants’ susceptibility score and age. A weak correlation that was not significant was found (*r* (91) = .02, *p* > .05). Susceptibility score is not related to age.

**Length of Employment.**

The mean knowledge score of participants’ from five different length of employment groupings were compared using a one-way ANOVA. No significant difference was found (F(4,90) = .774, *p* > .05). The participants’ from the five different employment length groups did not differ significantly in their knowledge score.

Table 16

*Knowledge Score - Mean and Standard Deviations for Length of Employment*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *n* | Mean Knowledge Score | Standard Deviation |
| Less than 1 year | 10 | 58.90 | 14.69 |
| 1 – 3 years | 14 | 59.36 | 10 |
| 4 – 6 years | 20 | 61.50 | 7.62 |
| 7 – 9 years | 12 | 57.58 | 5.93 |
| More than 10 years | 39 | 57.13 | 9.22 |

The mean attitude score of participants’ from five different length of employment groupings were compared using a one-way ANOVA. No significant difference was found (F(4,90) = .696, *p* > .05). The participants’ from the five different employment length groups did not differ significantly in their attitude score.

Table 17

*Attitude Score - Mean and Standard Deviations for Length of Employment*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *N* | Mean Attitude Score | Standard Deviation |
| Less than 1 year | 10 | 67.20 | 8.61 |
| 1 – 3 years | 14 | 65.50 | 6.98 |
| 4 – 6 years | 20 | 66.00 | 5.52 |
| 7 – 9 years | 12 | 62.67 | 9.2 |
| More than 10 years | 39 | 64.46 | 7.24 |

The mean behavior score of participants’ from five different length of employment groupings were compared using a one-way ANOVA. No significant difference was found (F(4,90) = .13, *p* > .05). The participants’ from the five different employment length groups did not differ significantly in their behavior score.

Table 18

*Behavior Score - Mean and Standard Deviations for Length of Employment*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *N* | Mean Behavior Score | Standard Deviation |
| Less than 1 year | 10 | 61.80 | 9.28 |
| 1 – 3 years | 14 | 63.14 | 7.68 |
| 4 – 6 years | 20 | 63.00 | 5.96 |
| 7 – 9 years | 12 | 61.75 | 9.48 |
| More than 10 years | 39 | 61.95 | 7.68 |

The mean susceptibility score of participants’ from five different length of employment groupings were compared using a one-way ANOVA. No significant difference was found (F(4,90) = .47, *p* > .05). The participants’ from the five different employment length groups did not differ significantly in their susceptibility score.

Table 19

*Susceptibility Score - Mean and Standard Deviations for Length of Employment*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *n* | Mean Susceptibility Score | Standard Deviation |
| Less than 1 year | 10 | 20.61 | 16.84 |
| 1 – 3 years | 14 | 20.56 | 12.87 |
| 4 – 6 years | 20 | 19.17 | 9.75 |
| 7 – 9 years | 12 | 23.89 | 13.29 |
| More than 10 years | 39 | 23.03 | 11.7 |

**Education.**

The mean knowledge score of participants’ from five different education levels were compared using a one-way ANOVA. No significant difference was found (F(4,90) = .27, *p* > .05). The participants’ from the five different education levels did not differ significantly in their knowledge score.

Table 20

*Knowledge Score - Mean and Standard Deviations for Education*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *N* | Mean Knowledge Score | Standard Deviation |
| High School Diploma | 10 | 56.50 | 10.29 |
| Associate’s Degree | 12 | 59.00 | 12.91 |
| Bachelor’s Degree | 41 | 59.32 | 8.99 |
| Master’s Degree | 25 | 57.76 | 8.52 |
| Terminal Degree | 7 | 60.00 | 7.94 |

The mean attitude score of participants’ from five different education levels were compared using a one-way ANOVA. No significant difference was found (F(4,90) = 2.4, *p* > .05). The participants’ from the five different education levels did not differ significantly in their attitude score.

Table 21

*Attitude Score - Mean and Standard Deviations for Education*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *N* | Mean Attitude Score | Standard Deviation |
| High School Diploma | 10 | 58.90 | 10.6 |
| Associate’s Degree | 12 | 67.42 | 6.54 |
| Bachelor’s Degree | 41 | 65.66 | 6.77 |
| Master’s Degree | 25 | 64.88 | 6.15 |
| Terminal Degree | 7 | 66.14 | 6.59 |

The mean behavior score of participants’ from five different education levels were compared using a one-way ANOVA. No significant difference was found (F(4,90) = 1.40, *p* > .05). The participants’ from the five different education levels did not differ significantly in their behavior score.

Table 22

*Behavior Score - Mean and Standard Deviations for Education*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *N* | Mean Behavior Score | Standard Deviation |
| High School Diploma | 10 | 58.80 | 10.46 |
| Associate’s Degree | 12 | 66.17 | 8.92 |
| Bachelor’s Degree | 41 | 61.73 | 7.14 |
| Master’s Degree | 25 | 62.76 | 6.43 |
| Terminal Degree | 7 | 62.43 | 6.68 |

The mean susceptibility score of participants’ from five different education levels were compared using a one-way ANOVA. No significant difference was found (F(4,90) = 1.04, *p* > .05). The participants’ from the five different education levels did not differ significantly in their susceptibility score.

Table 23

*Susceptibility Score - Mean and Standard Deviations for Education*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *N* | Mean Susceptibility Score | Standard Deviation |
| High School Diploma | 10 | 28.22 | 16.25 |
| Associate’s Degree | 12 | 18.00 | 14.18 |
| Bachelor’s Degree | 41 | 21.27 | 11.51 |
| Master’s Degree | 25 | 22.00 | 10.56 |
| Terminal Degree | 7 | 20.24 | 11.28 |

**Weekly Hours Worked.**

A Pearson correlation was calculated examining the relationship between participants’ knowledge score and average weekly hours worked. A weak correlation that was not significant was found (*r* (92) = .03, *p* > .05). Knowledge score is not related to hours worked.

A Pearson correlation was calculated examining the relationship between participants’ attitude score and average weekly hours worked. A weak correlation that was not significant was found (*r* (92) = -.05, *p* > .05). Attitude score is not related to hours worked.

A Pearson correlation was calculated examining the relationship between participants’ behavior score and average weekly hours worked. A weak correlation that was not significant was found (*r* (92) = .05, *p* > .05). Behavior score is not related to hours worked.

A Pearson correlation was calculated examining the relationship between participants’ susceptibility score and average weekly hours worked. A weak correlation that was not significant was found (*r* (92) = - .05, *p* > .05). Susceptibility score is not related to hours worked.

**Industry.**

An independent sample t test was calculated comparing the mean knowledge score of participants who worked in the technology industry to the mean knowledge score of participants who did not work in the technology industry. No significant difference was found (*t* (93) = - .22, *p* > .05). The mean knowledge score of those in technology (*M* = 58.96, *sd* = 9.84) was not significantly different from the mean of those not in technology (*M* = 58.49, *sd* = 9.24).

An independent sample t test was calculated comparing the mean attitude score of participants who worked in the technology industry to the mean attitude score of participants who did not work in the technology industry. No significant difference was found (*t* (93) = - .53, *p* > .05). The mean attitude score of those in technology (*M* = 65.63, *sd* = 6.22) was not significantly different from the mean of those not in technology (*M* = 64.75, *sd* = 7.66).

An independent sample t test was calculated comparing the mean behavior score of participants who worked in the technology industry to the mean behavior score of participants who did not work in the technology industry. No significant difference was found (*t* (93) = .24, *p* > .05). The mean behavior score of those in technology (*M* = 62, *sd* = 7.12) was not significantly different from the mean of those not in technology (*M* = 62.43, *sd* = 7.88).

An independent sample t test was calculated comparing the mean susceptibility score of participants who worked in the technology industry to the mean susceptibility score of participants who did not work in the technology industry. No significant difference was found (*t* (93) = .19, *p* > .05). The mean susceptibility score of those in technology (*M* = 21.34, *sd* = 11.2) was not significantly different from the mean of those not in technology (*M* = 21.85, *sd* = 12.62).

A detailed table of means and standard deviations by industry are presented in Appendix H. It should be noted that many of the industry choices contained few responses.

**Training.**

The mean knowledge score of participants who received different amounts of cybersecurity awareness training were compared using a one-way ANOVA. No significant difference was found (F(4,90) = 2.38, *p* > .05). The participants who received different amounts of cybersecurity awareness training did not differ significantly in their knowledge score. However, a positive directional trend can be observed in which more training results in a higher knowledge score.

Table 24

*Knowledge Score - Mean and Standard Deviations for Training on Average Per Year*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *N* | Mean Knowledge Score | Standard Deviation |
| No Training | 39 | 56.96 | 8.59 |
| One Time | 30 | 57.10 | 8.60 |
| Two Times | 6 | 59.17 | 13.88 |
| Three Times | 7 | 62.57 | 7.59 |
| More than 3 Times | 13 | 64.77 | 10.01 |

The mean attitude score of participants who received different amounts of cybersecurity awareness training were compared using a one-way ANOVA. No significant difference was found (F(4,90) = 2.06, *p* > .05). The participants’ who received different amounts of cybersecurity awareness training did not differ significantly in their attitude score.

Table 25

*Attitude Score - Mean and Standard Deviations for Training on Average Per Year*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *N* | Mean Attitude Score | Standard Deviation |
| No Training | 39 | 64.10 | 7.16 |
| One Time | 30 | 63.30 | 7.41 |
| Two Times | 6 | 67.00 | 7.48 |
| Three Times | 7 | 68.57 | 5.68 |
| More than 3 Times | 13 | 68.77 | 6.60 |

The mean behavior score of participants’ who received different amounts of cybersecurity awareness training were compared using a one-way ANOVA. No significant difference was found (F(4,90) = 2.44, *p* > .05). The participants’ who received different amounts of cybersecurity awareness training did not differ significantly in their behavior score. However, a positive directional trend can be observed in which more training results in a higher behavior score.

Table 26

*Behavior Score - Mean and Standard Deviations for Training On Average Per Year*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *N* | Mean Behavior Score | Standard Deviation |
| No Training | 39 | 60.72 | 6.98 |
| One Time | 30 | 61.07 | 8.28 |
| Two Times | 6 | 64.83 | 6.52 |
| Three Times | 7 | 66.86 | 5.37 |
| More than 3 Times | 13 | 66.31 | 7.77 |

The mean susceptibility score of participants’ who received different amounts of cybersecurity awareness training were compared using a one-way ANOVA. A significant difference was found among those with varying levels of cybersecurity awareness training (F(4,90) = 2.78, *p* < .05). However, both Tukey’s HSD and Duncan’s post hoc tests showed no differences among the groups. As a result, the LSD post hoc procedure was run with an adjustment to the alpha level needed to achieve statistical significance downward by dividing the original alpha (.05) by the ten comparisons that were made. This created a new alpha level of .005. No significant differences could be found after making that adjustment. However, a negative directional trend can be observed in which more training results in a lower susceptibility score.

Table 27

*Susceptibility Score - Mean and Standard Deviations for Training On Average Per Year*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *n* | Mean Susceptibility Score | Standard Deviation |
| No Training | 39 | 24.02 | 11.01 |
| One Time | 30 | 24.18 | 12.30 |
| Two Times | 6 | 18.89 | 12.50 |
| Three Times | 7 | 15.00 | 9.63 |
| More than 3 Times | 13 | 13.97 | 13.15 |

**Training (Recode).**

Because a significant difference was found in the previous analysis on training and a negative directional trend was observed in relation to training and susceptibility score, the training variable was recoded into three groups: no training, training received one to three times on average for the year, and training received more than three times on average during the year. This recode allowed for better exploration of the participant groups based on what can be perceived as no training, some training, or a lot of training, respectively.

The mean knowledge score of participants’ who received different amounts of cybersecurity awareness training were compared using a one-way ANOVA. A significant difference was found among those who received different amounts of training (*F*(2, 92) = 3.65, *p* < .05). Tukey’s HSD was used to determine the nature of the difference between the different amounts of training. This analysis revealed that participants who received cybersecurity training more than three times on average for per year scored significantly (*p* < .05) higher (*M* = 64.77, *sd* = 10.01) than participants who received no training (*M* = 56.95, *sd* = 8.59). Participants who received training between one and three times on average per year (*M* = 58.28, *sd* = 9.29) were not significantly different from either of the other two groups.

Table 28

*Knowledge Score - Mean and Standard Deviations for Training (Recode) on Average Per Year*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *N* | Mean Knowledge Score | Standard Deviation |
| No Training | 39 | 56.95 | 8.59 |
| 1 -3 Times | 43 | 58.28 | 9.29 |
| More than 3 Times | 13 | 64.77 | 10.01 |

The mean attitude score of participants’ who received different amounts of cybersecurity awareness training were compared using a one-way ANOVA. No significant difference was found (F(2, 92) = 2.14, *p* > .05). The participants’ who received different amounts of cybersecurity awareness training did not differ significantly in their attitude score. However, a positive directional trend can be observed in which more training results in a higher attitude score.

Table 29

*Attitude Score - Mean and Standard Deviations for Training (Recode) on Average Per Year*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *n* | Mean Attitude Score | Standard Deviation |
| No Training | 39 | 64.10 | 7.16 |
| 1 -3 Times | 43 | 64.67 | 7.34 |
| More than 3 Times | 13 | 68.77 | 6.60 |

The mean behavior score of participants’ who received different amounts of cybersecurity awareness training were compared using a one-way ANOVA. No significant difference was found (F(2, 92) = 2.75, *p* > .05). The participants’ who received different amounts of cybersecurity awareness training did not differ significantly in their behavior score. However, a positive directional trend can be observed in which more training results in a higher behavior score.

Table 30

*Behavior Score - Mean and Standard Deviations for Training (Recode) on Average Per Year*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *n* | Mean Behavior Score | Standard Deviation |
| No Training | 39 | 60.72 | 6.98 |
| 1 -3 Times | 43 | 62.53 | 7.87 |
| More than 3 Times | 13 | 66.31 | 7.77 |

The mean susceptibility score of participants’ who received different amounts of cybersecurity awareness training were compared using a one-way ANOVA. A significant difference was found among those who received different amounts of training (*F*(2, 92) = 3.51, *p* < .05). Tukey’s HSD was used to determine the nature of the difference between the different amounts of training. This analysis revealed that participants who received cybersecurity training more than three times on average for per year had a significantly *(p* < .05) lower susceptibility score (*M* = 13.97, *sd* = 13.16) than participants who received no training (*M* = 24.02, *sd* = 11.01). Participants who received training between one and three times on average per year (*M* = 21.95, *sd* = 12.21) were not significantly different from either of the other two groups.

Table 31

*Susceptibility Score - Mean and Standard Deviations for Training (Recode) on Average Per Year*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *n* | Mean Susceptibility Score | Standard Deviation |
| No Training | 39 | 24.02 | 11.01 |
| 1 -3 Times | 43 | 21.95 | 12.21 |
| More than 3 Times | 13 | 13.97 | 13.16 |

**Rank.**

An independent sample t test was calculated comparing the mean knowledge score of non-owners / non-highest ranking officials to the mean knowledge score of owners / highest ranking officials. No significant difference was found (*t* (93) = - 1.26, *p* > .05). The mean knowledge score of non-owners / non-highest ranking officials (*M* = 57.00, *sd* = 9.1) was not significantly different from the mean of owners / highest ranking officials (*M* = 59.52, *sd* = 9.45).

An independent sample t test was calculated comparing the mean attitude score of non-owners / non-highest ranking officials to the mean attitude score of owners / highest ranking officials. No significant difference was found (*t* (93) = - .71, *p* > .05). The mean attitude score of non-owners / non-highest ranking officials (*M* = 64.29, *sd* = 6.75) was not significantly different from the mean of owners / highest ranking officials (*M* = 65.39, *sd* = 7.55).

An independent sample t test was calculated comparing the mean behavior score of non-owners / non-highest ranking officials to the mean behavior score of owners / highest ranking officials. No significant difference was found (*t* (93) = - .54, *p* > .05). The mean behavior score of non-owners / non-highest ranking officials (*M* = 61.74, *sd* = 6.15) was not significantly different from the mean of owners / highest ranking officials (*M* = 62.62, *sd* = 8.38).

An independent sample t test was calculated comparing the mean susceptibility score of non-owners / non-highest ranking officials to the mean susceptibility score of owners / highest ranking officials. No significant difference was found (*t* (93) = .96, *p* > .05). The mean susceptibility score of non-owners / non-highest ranking officials (*M* = 23.32, *sd* = 10.78) was not significantly different from the mean of owners / highest ranking officials (*M* = 20.81, *sd* = 12.89).

**Cultural Identity.**

An independent sample t test was calculated comparing the mean knowledge score of those who identified as non-American to the mean knowledge score of participants’ who identified as American. No significant difference was found (*t* (93) = - .66, *p* > .05). The mean knowledge score of participants who identified as non-American (*M* = 56.17, *sd* = 12.66) was not significantly different from the mean of participants who identified as American (*M* = 58.79, *sd* = 9.17).

An independent sample t test was calculated comparing the mean attitude score of those who identified as non-American to the mean attitude score of participants’ who identified as American. No significant difference was found (*t* (93) = .93, *p* > .05). The mean attitude score of participants who identified as non-American (*M* = 67.67, *sd* = 8.04) was not significantly different from the mean of participants who identified as American (*M* = 64.82, *sd* = 7.22).

An independent sample t test was calculated comparing the mean behavior score of those who identified as non-American to the mean attitude score of participants’ who identified as American. No significant difference was found (*t* (93) = .23, *p* > .05). The mean behavior score of participants who identified as non-American (*M* = 67.67, *sd* = 8.04) was not significantly different from participants who identified as American (*M* = 64.82, *sd* = 7.22).

An independent sample t test was calculated comparing the mean susceptibility score of those who identified as non-American to the mean susceptibility score of participants’ who identified as American. No significant difference was found (*t* (93) = -.10, *p* > .05). The mean susceptibility score of participants who identified as non-American (*M* = 21.2, *sd* = 11.81) was not significantly different from participants who identified as American (*M* = 21.74, *sd* = 12.27).

**Chapter V**

**Discussion**

**Introduction**

This discussion explains a brief review of the research study, an explanation of the results in the context of current literature, implications, limitations, suggestions for future research, and a conclusion.

**Summary**

The purpose of this research study was to answer the following question: *How do demographic characteristics, including gender, age, education, length of employment with a company, hours worked, industry, training, rank, and cultural identity, of employees in small businesses in Northeastern Pennsylvania predict social engineering susceptibility?* This study was conducted using the Human Aspects of Information Security Questionnaire (HAIS-Q) created by Parsons et al. (2014) which measures information security awareness. Each participant received an information security awareness score which was then converted to a social engineering susceptibility score with the understanding that the higher information security awareness, the lower the susceptibility to social engineering (Stewart & Jurjens, 2016; Pyzik, 2015; Janczewski & Fu, 2010).

The survey was open for eight weeks and 95 respondents representing owners and employees of small businesses in Northeastern Pennsylvania participated. The hypothesis addressed in this study is as follows:

H1: The demographic characteristics of employees in small business including age, gender, education, length of employment with a company, hours worked, training, and cultural identity, predict susceptibility to social engineering.

The results of this study did not support H1, but rather, the null hypothesis was supported: The demographic characteristics of employees in small business including age, gender, education, length of employment with a company, hours worked, training, and cultural identity, *do not* predict susceptibility to social engineering.

**Discussion**

This research study did not find that any of the demographic characteristics measured in the survey were able to predict susceptibility to social engineering. While the other studies noted in the literature were not conducted on small business owners and employees, the findings from this study were in contradiction to some previous findings which found that woman more than men were susceptible to social engineering attempts (Sheng et al., 2010; Jagatic et al., 2007, Halevi et al., 2015, Algarni et al., 2015) and to another study which found that men more than woman were susceptible to social engineering attempts (Happ et al., 2016). This study was not able to clarify or confirm their findings, and one reason could be because of the population studied. This study was unique in that it was conducted in small businesses in northeastern Pennsylvania rather than on college students, faculty, or staff (Moody et al., 2017; Jagatic et al. 2007; Jansson & vonSolms, 2013; Vishwanath et al., 2011), other industries such as government (Parsons et al., 2013), or large companies in healthcare, retail, education, construction, and manufacturing (Parsons et al., 2014).

Moody et al. (2017) determined that age was not significant in predicting susceptibility to phishing attacks, and the results of this study support those findings. It should be noted that the age range of participants in this study (19 – 75) was different from the smaller range of college-age students included in that study. The research described here, however, is in contradiction to the study by Sheng et al. (2010) which determined that those in the age range of 18 - 25 were more likely to fall victim to a phishing scam.

While cybersecurity awareness training was found to not be a significant predictor of social engineering susceptibility, a positive directional trend can be found in knowledge and behavior scores when more training is received by employees. Consequently, a negative directional trend can be found in susceptibility scores when more training is received by employees. Because of these trends, the researcher explored the training variable by grouping responses in a different way. In the demographic section of the questionnaire, participants were asked to think about the last three years and report how many times, on average per year, they received cybersecurity awareness training. After grouping responses together to run analysis on those who received no training, those who received training on average one to three times per year, and those received training on average more than three times per year, a significant difference was found in the knowledge score and overall susceptibility score between those who received no training and those who received training more than three times per year. These results support previous findings by Airehrour et al. (2018) and Heartfield & Loukas (2015) that awareness training has a substantial impact in mitigating social engineering attempts. This is an important concept for small businesses owners to consider as part of their information security plan, if one exists. Awareness training can have a significant impact on employees of small businesses and help them if a social engineering attack is attempted.

The supplemental analysis in this research study shows that significance was found in terms of the three categories found in the HAIS-Q: knowledge, attitude, and behavior. Knowledge has been shown to be a significant predictor of attitude and attitude has been shown to be a significant predictor of behavior. Both knowledge and attitude have been shown to be significant predictors of behavior. These results support the findings and the hypothesis proposed by Parsons et al. (2014) in which knowledge of information security policies leads to a better attitude towards these policies. In addition, increased knowledge and attitude support less risky behavior as measured by a self-report mechanism. Their findings and those described here provide support for their HAIS Model, specifically the knowledge, attitude, and behavior (KAB) component.

The results are important in the context of the population studied here because small businesses should be encouraged to increase employees’ knowledge of cybersecurity and social engineering issues in order to impact attitude, and most importantly, to influence their behaviors in the workplace. Small business owners and managers should attempt to determine how they can make their employees more knowledgeable if they want to see them display appropriate behaviors when faced with a social engineering attempt.

The training variable is a unique demographic characteristic since it is one that can be easily changed unlike gender, age, or cultural identity. To alter a participants’ response to the training question, one simply has to provide training to the employee. The significance of this variable was not apparent in the multiple regression analysis but later became apparent when ANOVAs were analyzed on the three different options: no training, some training, and a lot of training.

Two of the variables studied in this research, cultural identity and industry, did not receive enough responses in any of the response categories to thoroughly make a determination as to the significance of these variables on social engineering susceptibility. The survey could be expanded to better capture the cultural identity of participants in a more culturally diverse population rather than northeastern Pennsylvania to determine if there is support for prior research findings on the importance of culture (Bullee et al., 2015; Butavicius et al., 2017; Williams et al., 2018).

This study helped to fill a gap in the published social engineering research since it studied the small business population. As previously stated, small businesses comprise the majority of businesses in the United States (SBA.gov, 2018) and a successful social engineering attack on these businesses can be detrimental to the ability of the organizations to withstand an attack of this type (LeClair, 2015).

Even though none of the demographic variables studied here have been found to be significant predictors of social engineering susceptibility, these findings have major implications for the future of small businesses and how they choose to proceed in protecting themselves, if at all, from social engineering attacks.

**Implications**

The results of this study suggest that demographic characteristics of employees in small business are not significant predictors of social engineering susceptibility. This can provide some reassurance to small business owners that they and their employees are not more or less susceptible to social engineering attacks based on their demographic characteristics measured here, most of which are out of the control or at least limited control of the owner or employee. These results suggest that there is something else that contributes to social engineering susceptibility, possibly something better able to be controlled by the owner or employee. Small businesses should not view some employees as more of a risk than others simply based on their demographic characteristics. Other contributing factors to susceptibility, rather than demographics, could include the psychological characteristics described earlier such as fear of losing / eagerness to gain (Goel et al., 2017; Cheung-Blunden et al., 2018), likability and trust (Flores et al., 2013; Guadagno, et al., 2013), and boredom proneness (Moody et al., 2017). In addition, Cialdini’s (2007) principles of persuasion could be a contributing factor. Referring to the conceptual framework (See Figure 3), the impact of these qualities on the various demographic characteristics could be studied to determine if the persuasion principles have any influence on susceptibility to social engineering.

Participants had a possible information security awareness scores in the range of 45 – 225 with a lower score suggesting higher susceptibility to social engineering. Small business owners and employees in northeastern Pennsylvania scored relatively high on the information security awareness scores with less than 10% of the respondents (*n* = 9) scoring less than 161 points. Even though prior research suggests that 2/3 of small businesses are concerned about cybersecurity issues (Hiscox, 2018), information security awareness is relatively high in the small business population surveyed here. While this does not necessarily alleviate concerns they might have, it does offer some encouragement that small business might be more aware of cybersecurity issues than previously thought and can actively work toward ways to reduce the success of attacks on their business. This can include involving employees in creating an information security plan since most of them have a moderate level of information security awareness. The small number of employees in these businesses makes this a manageable solution to implement.

Because knowledge has been determined to be a significant predictor of attitude and attitude has been determined to be a significant predictor of behavior, small businesses should focus on ways to increase employee knowledge in an attempt to influence their behavior in terms of cybersecurity issues. Related to these findings, even though cybersecurity awareness training has not been found to be a significant predictor of social engineering susceptibility, those employees who received training more than three times per year on average have lower susceptibility scores than those employees who received no training.

Although small businesses usually operate on limited budgets and might not allocate funding towards training (Jackson, 2018), the results indicate that training employees on cybersecurity awareness could have an impact on their likelihood of falling victim to an attempted social engineering attack. Small business owners should consider various training options for their employees especially on a continuing basis several times per year since this can strengthen the information security protections of the company.

An important distinction should be made regarding the difference between information security awareness and information security awareness *training*. Awareness can simply consist of sending reminder emails to employees or posting memos in various office locations to encourage individuals to be mindful of potential social engineering attacks. Awareness training, however, is more involved because it includes these educational efforts while also being interactive. This type of training focuses more on modifying individual behaviors in the workplace rather than simply trying to enforce rules and regulations (Newcombe, 2016).

This issue of security awareness training is so crucial that its importance and relevance is seen through industry and even the United States government. The Department of Homeland Security promotes a solid connection between various industries and the government by supporting awareness campaigns such as National Cybersecurity Awareness Month in addition to encouraging active involvement in measures that can be undertaken by individuals and businesses to protect themselves from threats (Lindsey, 2019). Considering awareness training is a $1 billion per year industry and growing at a rate of 13% (Newcombe, 2016), the results of this research study align with the industry trends and support the growing need for awareness training in all businesses.

The conceptual framework that guided this research study (See Figure 3) was revisited after the study was complete. The cybersecurity framework in organizations was proposed to serve as a barrier between the principles of persuasion used in a social engineering attack and how they influenced the demographic characteristics of employees. It is possible that the owners and employees of the small businesses surveyed here had a cybersecurity framework in place. This data was not captured in the HAIS-Q or demographic questionnaire since it was outside the scope of this study, but it does provide another element for small businesses to think about. It was determined that something else, besides demographics, must contribute to social engineering susceptibility. Perhaps the principles of persuasion and how a cybersecurity framework functions in a business could help small business owners better understand their susceptibility to social engineering. If there is no cybersecurity framework in place, the NCCIC Cybersecurity Framework (See Figure 2) could be a potential option for small businesses because of its simplicity and ease of implementation.

**Limitations**

The researcher has identified limitations in this study. Survey questions are designed to capture data relating to employee’s knowledge, attitude, and behavior through a self-report mechanism. Caution should be used when interpreting self-report items due to social desirability bias which is the desire to answer questions in ways that are considered by the respondent to be socially accepted especially if the questions involve profound information that could reflect on an individual’s life or work ethic (Social Desirability Bias, 2004). While a fabricated social engineering attempt would have provided a more robust mechanism to capture employee knowledge, attitude, and behavior, it was not feasible considering the quantity of small businesses and industries that the researcher wanted to study.

The number of respondents within each industry was out of the control of the researcher and could be impacted by a number of different reasons including seasonality of workload, time of year the survey was sent, and employee interest in participating in a non-work related activity. This study assumed that participants who completed the survey did so at their own volition and without the assistance of anyone else. Data was analyzed on the assumption that employees understood the questions being asked and answered honestly without thinking about the implications of their answers and how the data captured would reflect on them or their companies.

The HAIS-Q used in the research study can be considered a limitation since the original intent of the questionnaire was to measure information security awareness and not social engineering susceptibility. To the best of the researcher’s knowledge, there is no specific tool that exists to measure social engineering susceptibility. However, the researcher has made the assumption that social engineering susceptibility is comprised of the knowledge, attitude, and behavior of employees as measured in the HAIS-Q. Since the HAIS-Q has been tested for validity and reliability, it is a solid tool to measure the three components that lead someone to fall for social engineering attacks.

Awareness has been suggested to mitigate social engineering attacks (Pyzik, 2015), and it has also been shown to increase employees’ positive attitudes towards information security procedures. Increased awareness leads to a reduction in the occurrence of potentially risky behavior that might impact information security (Parsons et al., 2014). In addition, low information security awareness has been shown to contribute to successful social engineering attacks (Janczewski & Fu, 2010). As a result, a logical inference would be that the higher the score on the HAIS-Q (meaning higher information security awareness), the lower the employee’s susceptibility to social engineering.

This study focused only on small businesses with less than 25 employees in northeastern Pennsylvania. As a result of the small, limited group that was studied, it may be difficult to generalize the findings in this study to the larger population, different geographic regions, or industries not mentioned here. This is apparent in the demographic section of the questionnaire in which more than 93.7% of respondents (*n* = 89) identified as American and more than 38.9% of respondents (*n* = 37) selected *other* as their current industry.

**Future Research**

This research study contributed to the literature on social engineering especially to the literature on a critical but under-researched population of small businesses. However, this study highlights areas for future research on the topic. The HAIS-Q is suggested to continue to be used in other populations to determine if it is an accurate tool to predict social engineering susceptibility. It has been utilized in industries such as government (Parsons et al., 2013), healthcare, retail, education, construction, and manufacturing (Parsons et al., 2014), and in small businesses as part of this research. It would be interesting and beneficial to provide this survey to a larger number of employees working in a single industry or repeat the use of the HAIS-Q in a more diverse, geographic region.

This study found areas of significance that require further research and explanation. Awareness training for employees was not found to be a significant predictor of social engineering susceptibility. However, training did show significance and a positive directional trend was observed in the data suggesting that more training results in a higher knowledge and behavior score. In the supplementary exploration, a negative directional trend was observed in the data suggesting that more training results in a lower susceptibility score. Further research is suggested to confirm or explain these findings. In addition, the regression analysis for education showed conflicting significance values in which the ANOVA was not significant, but the multivariate regression coefficients showed significance for the two education dummy variables. Further research is needed to clarify these results.

Businesses are viewing social engineering as a converged threat (Aleem et al., 2013) including accounting firms KPMG and PwC. They have found that security violations are usually a combination of failures on the part of systems, processes, and people (Aleem, et al, 2013). Airehrour et al. (2018) reported on PwC surveys indicating that over 90% of financial organizations have experienced a cyberattack in some form, and the trend is for cyberattacks to become much more prevalent in the industry in the years to come. This survey utilizing the HAIS-Q can be used in conjunction with other social engineering tests that focus on systems since this survey has focused on the people and processes in organizations. This multi-faceted approach can target this converged threat to create a more robust protection plan for organizations today, especially in the case of the accounting firms mentioned here that have already recognized and experienced the significant impact of cyberattacks.

Other methods can be utilized to validate the results found in this survey such as conducting fabricated social engineering attempts on these small business owners and employees. Studies have been conducted with fabricated phishing emails to study susceptibility to social engineering (Jansson & von Solms, 2013; Goel, et al., 2017). Similar studies can be repeated by sending fictitious phishing emails to the small business population studied here and observing and measuring their behavior in response to receiving the emails. Measurements can include whether they clicked on links, opened attachments, or complied with requests in the email. An additional step in the research process to further validate the results of this study would be to attempt to increase the knowledge of employees by offering cybersecurity awareness training in between fabricated phishing attempts to determine if increased knowledge as a result of training really does impact employee behavior.

Employees and owners of small businesses who did not have company email addresses were not allowed to participate in this research study even though they have the potential to be targets of social engineering attacks. This excluded population is one that should be studied in future research, perhaps with a different mechanism than the HAIS-Q. Fabricated social engineering attempts can be applied to this population but with the use of in-person requests or phone calls rather than email.

Other survey mechanisms can be considered to determine whether the HAIS-Q is an appropriate tool to use to measure social engineering susceptibility and whether there is a valid link that can be made between information security awareness and social engineering susceptibility. Other surveys can be given to this same small business population and results can be compared to the results found here to confirm that demographic characteristics do not predict social engineering susceptibility.

Even though the results suggest that demographic characteristics are not significant predictors of social engineering susceptibility, it is well-known that employees are susceptible to some extent based on the success of social engineering attacks. Future research may focus on trying to find what the other predictors of social engineering susceptibility are since demographic characteristics, according to this study, only account for 6.8% of an individual’s susceptibility to these types of attacks.

The conceptual framework described earlier can be revisited to expand the focus of future research. This study concentrated solely on the demographic characteristics and susceptibility to social engineering. Additional layers can be added to a study to determine if Cialdini’s (2007) principles of persuasion impact individuals with certain demographic characteristics and if those principles eventually impact susceptibility. Further analysis can include the implementation of a cybersecurity framework, such as the one depicted previously in this research by the National Cybersecurity and Communications Integration Center (NCCIC) from the United States Department of Homeland Security. Future research can determine if the combination of the persuasion principles, cybersecurity framework, and demographic characteristics can predict susceptibility to social engineering.

Another area of future research explores the changes posed to the insurance industry because of social engineering threats. These types of attacks can cost a business a substantial sum of money because of the possible interruption to business processes, public relations and legal fees, loss of sales, and the research needed to fully understand the attack and mitigate any future attacks (Kandel & Selarnick, 2017). Companies will sometimes carry cyber liability insurance but what most companies are realizing when they file a claim, is that social engineering does not fall under the umbrella of what is covered for cyberattacks. The main reason for this gap in coverage is the fact that hackers do not directly break into a system or obtain information, but rather, they use an employee, or middleman, who takes some sort of action in order for that hacker to gain the access. The loss incurred on the business side as a result of actions of the employee who fell victim to the social engineering attack are not covered under typical insurance coverage (Dandelles & Liu, 2018; Bednar, 2018; Kandel & Selarnick, 2017). Research can be directed toward better understanding the link between social engineering and insurance coverage or perhaps used as another facet of security training in organizations. Not only do employees need to be trained on how to prevent successful attacks, but managers and decision makers of a company need to better understand their risk mitigation and insurance policies in the event that an attack does occur.

**Conclusion**

Social engineering attacks are become more common in today’s interconnected world on both an individual and a business level. When businesses are victims of social engineering attacks, the impact can be far-reaching and affect not only the business, but its customers, vendors, shareholders, and society as a whole. Small businesses comprise the majority of businesses in the United States and are not immune to the effects of social engineering. Demographic characteristics were studied to determine if they are significant predictors of social engineering susceptibility in owners and employees of small businesses in northeastern Pennsylvania. Even though demographics were not shown to be significant predictors, these findings have several implications for small businesses and how they can protect themselves from the growing threat of social engineering attacks.

**References**

Abawajy, J. (2014). User preference of cybersecurity awareness delivery methods.

*Behaviour & Information Technology, 33*(3), 236 – 247. Retrieved from Social

Sciences CitationIndex.

Aguilar, L. (2015). The need for greater focus on the cybersecurity challenges facing

small and midsize businesses. U.S. Securities and Exchange Commission. Retrieved

from https://www.sec.gov/news/statement/cybersecurity-challenges-for-small

midsize-businesses.html#\_edn6

Airehrour, D., Nair, N., & Madanian, S. (2018). Social engineering attacks and

countermeasures in the New Zealand banking system: Advancing a user-reflective

mitigation model. *Information, 9*(5), 10. doi: 10.3390/info9050110

Aleem, A., Wakefield, A., & Button, M. (2013). Addressing the weakest link:

Implementing converged security. *Security Journal*, 26(3), 236-248. doi:

10.1057/sj.2013.14

Algarni, A., Xu, T., & Chan, T. (2015). Susceptibility to social engineering in social

networking sites: The case of Facebook. *36th International Conference on*

*Information Systems (ICIS2015)*, 13-16. Retrieved from https://pdfs.semanticscholar.

org/055c/cd809b80a3d2e8e813acd81ddb98de8c3c7a.pdf?\_ga=2.165038463.174621

1815.1548784731-797035428.1548784731

Anderson, C., Baskerville, R., & Kaul, M. (2017). Information security control theory:

Achieving a sustainable reconciliation between sharing and protecting the privacy of

information. *Journal of Management Information Systems, 34*(4), 1082 – 1112. doi:

https://doi.org/10.1080/07421222.2017.1394063

Ashford, W. (2016). Social engineering is top hacking method, survey shows.

*ComputerWeekly.com*. Retrieved from https://www.computerweekly.com/news/

4500272941/Social-engineering-is-top-hacking-method-survey-shows

Bednar, J. (2018). Lines of defense: Cyber threats are a fact of life for businesses.

*Business West, 35*(11), 34 – 38. Retrieved from Regional Business News Database.

Bullee, J., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of

social engineering attacks: A literature-based dissection of successful attacks. *Journal*

*of* *Investigative Psychology and Offender Profiling, 15*(1), 20 – 45. Retrieved from

Social Sciences Citation Index.

Bullee, J., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2015). The persuasion and

security awareness experiment: Reducing the success of social engineering attacks.

*Journal of Experimental Criminology*, *11*, 97-115. doi: 10.1007/s11292-014-9222-7

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015). Breaching the

human firewall: Social engineering in phishing and spear-phishing emails.

*Australasian Conference on Information Systems*. Retrieved from https://www.

reserachgate.net/publications/303812216\_Breaching\_the\_Human\_Firewall\_

Social\_engineering\_in\_Phishing\_and\_Spear-Phishing\_Emails

Carlton, M. & Levy, Y. (2017). Cybersecurity skills: Foundational theory and the

cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of*

*Applied Knowledge* *Management, 5*(2). Retrieved from https://www.researchgate.

net/publication/318276855\_Cybersecurity\_skills\_Foundational\_theory\_and\_the\_

cornerstone\_of\_advanced\_persistent\_threats\_APTs\_mitigation/link/595f8bfba6fdc

cc9b1b02583/download

Cheung-Blunden, V., Cropper, K., Panis, A., & Davis, K. (2018). Functional divergence

of two threat-induced emotions: Fear-based versus anxiety-based cybersecurity

preferences. *Emotion.*  https://doi.org/10.1037/emo0000508

Cialdini, R. (2007). *Influence: The Psychology of Persuasion*. New York, NY. Harper

Collins.

Dandelles, S. & Liu, J. (2018). Insurance coverage for social engineering scams under

review. *Property & Casualty 360, 122*(3), 16 – 17. Retrieved from Business Source

Premier.

Dawson, J. & Thomson, R. (2018). The future cybersecurity workforce: Going beyond

technical skills for successful cyber performance. *Frontiers in Psychology, 9*(744).

doi: 10.3389/fpsyg.2018.00744

Elifoglu, I., Abel, I., & Tasseven, O. (2018). Minimizing insider threat risk with

behavioral monitoring. *Interdisciplinary Journal on Risk and Society, (38)*, 2, 61 –

73. Retrieved from EBSCO Host Database.

Fan, W., Lwakatare, K., Rong, R. (2017). Social engineering: I-E based model of human

weakness for attack and defense investigations. *Computer Network and Information*

*Security, 1*, 1-11. doi: 10.5815/ijcnis.2017.01.01

Federal Bureau of Investigation, (2018). *Internet crime complaint center*. Retrieved from

https:/www.ic3.gov

Flores, W., Holm, H., Svensson, G., Ericsson, G. (2013). Using phishing experiments and

scenario-based surveys to understand security behavior. *Information Management*

*and Computer Security, 22*(4), 393-406. doi: 10.1108/IMCS-11-2013-0083

Fowler, F. (2009). *Survey Research Methods,* 4th edition, Volume 1. Thousand Oaks, CA.

Sage Publications.

FSB. (2016). Cyber resilience: How to protection small firms in the digital economy.

Retrieved from https://www.fsb.org.uk/docs/default-source/fsb-org-uk/FSB-Cyber

Resilience-report2016.pdf?sfvrsn=0

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human

vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44.

Retrieved from Academic Search Premier.

Guadagno, R., Muscanell, N., Rice, L., Roberts, N. (2013). Social influence online: The

impact of social validation and likability on compliance. *Psychology of Popular*

*Media Culture,* *2*(1), 51 -60. doi: 10.1037/a0030592

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study

of personality, phishing self-efficacy, and vulnerability to spear-phishing. *SSRN*

*Electronic* *Journal,* doi: 10.2139/ssrn.2544742

Happ, C., Melzer, A., & Steffgen, G. (2016). Trick with treat – Reciprocity increases the

willingness to communicate personal data. *Computers in Human Behavior, 61*, 372

377. http://dx.doi.org/10.1016/j.chb.2016.03.026

Harris, S. (2018). Cyber security threats against small businesses on the rise in 2018.

*Idaho State Journal*

Hasle, H., Kristiansen, Y., Kintel, K., & Snekkenes, E. (2005). Measuring resistance to

social engineering. *Information Security Practice & Experience.* *3439*, 132-143.

Lecture Notes in Computer Science. DOI: 10.1007/978-3-540-31979-5\_12

Heartfield, R. & Loukas, G. (2015). A taxonomy of attacks and a survey of defense

mechanisms for semantic social engineering attacks. *ACM Computing Surveys, 48*(3),

doi: 10.1145/2835375

Heartfield, R., Loukas, G., & Gan, D. (2016). You are probably not the weakest link:

Towards practical prediction of susceptibility to semantic social engineering attacks.

*IEEE Access,* (4), 6910-6928. Doi: 10.1109/access.2016.2616285

Hsu, C., Lee, J., & Straub, D. (2012). Institutional influences on information systems

security innovations. *Information Systems Research, 23*(3), 918 – 939. doi: 10.12878/

isre.1110.0393

Hiscox (2018). Small business cyber risk report. Retrieved from https://www.hiscox.

com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf

Ifinedo, P. (2016). Critical times for organizations: What should be done to curb workers’

noncompliance with IS security policy guidelines? *Information Systems Management,*

*33*(1), 30 – 41. http://dx.doi.org/10.1080/10580530.2015.1117868

InfoSec Institute (n.d). The top ten most famous social engineering attacks. Retrieved

from https://resources.infosecinstitute.com/the-top-ten-most-famous-social

engineering-attacks/#gref

Jackson, R. (2018). Pulling strings. *Internal Auditor, 75*(4), 34 – 39. Retrieved from

Business Source Premier.

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing.

*Communications of the ACM, 50*(10), 94 – 100. doi: 10.1145/1290958.1290968.

Janczewski, L. & Fu, L. (2010). Social engineering-based attacks: Model and New

Zealand perspective. *Proceedings of the International Multiconference on Computer*

*Science and* *Information Technology*. Retrieved from https://annalscsis.org/

proceedings/2010/pliks/36.pdf

Jansson, K. & von Solms, R. (2013). Phishing for phishing awareness. *Behavior &*

*Information Technology, 32*(6), 584-593. doi: 10.1080/0144929X.2011.632650

Kandel, E. & Selarnick, A. (2017). Insuring against social engineering attacks. *Risk*

*Management, 64*(4), 12. Retrieved from Biography in Context Database.

Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information

security: An empirical study of intentional versus actual behavior. *Information*

*Management & Computer* *Security, 21*(1), 5-15. doi: 10.1108/09685221311314383

Leary, J. (2016). The biggest data breaches in 2016. *Identity Force*. Retrieved from

https://www.identityforce.com/blog/2016-data-breaches

LeClair, J. (2015). Testimony before U.S. House of Representatives. Retrieved from

https://docs.house.gov/meetings/SM/SM00/20150422/103276/HHRG-114-SM00

20150422-SD003-U4.pdf

Let’s talk about social engineering small businesses. (2018). *Social-Engineer.* Retrieved

from https://www.social-engineer.com/lets-talk-about-social-engineering-small

businesses/

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of*

*Psychology.140*(22), 5-55. Retrieved from https://legacy.voteview.com/pdf/Likert\_

1932.pdf

Lindsey, N. (2019). Organizations are embracing cyber security awareness training as the

first line of defense against hackers. *CPO Magazine.* Retrieved from

https://www.cpomagazine.com/cyber-security/organizations-are-embracing-cyber

security-awareness-training-as-the-first-line-of-defense-against-hackers

Lineberry, S. (2007). The human element: The weakest link in information security.

*Journal of Accountancy*. Retrieved fromhttps://www.journalofaccountancy.com/

issues /2007/nov/thehumanelementtheweakestlinkininformationsecurity.html

McCrae, R. & John, O. (1992). An introduction to the five-factor model and its

applications. *Journal of Personality, 60*(2), 175-215. http://dx.doi.org/10.1111/j.1467

6494.1992.tb00970.x

Meng, R. & Jun, Y. (2017). 360 degrees of social influence: How others’ presence,

attitudes, and behaviors change the way we think and behave. *Advances in Consumer*

*Research*, *45*, 181 – 185. Retrieved from Business Source Premier.

Merriam-Webster Online Dictionary. Retrieved from https://www.merriam

webster.com/dictionary/industry

Mitnick, K. & Simon, W. (2003). *The art of deception*. Indianapolis, IN. Wiley.

Moody, G., Galletta, D., & Dunn, B. (2017). Which phish get caught? An exploratory

study of individuals’ susceptibility to phishing. *European Journal of Information*

*Systems, 26*, (6), 564 – 584. https://doi.org/10.1057/s41303-017-0058-x

Muscanell, N., Guadagno, R., & Murphy, S. (2014). Weapons of influence misused: A

social influence analysis of why people fall prey to internet scams. *Social and*

*Personality* *Psychology Compass, 8*(7), 388-396. https://doi.org/10.1111/spc3.12115

Nekoranec, J. (2013). Management and organizational behavior: Some basic aspects.

*Journal of Defense Resources Management, 4*(1), 93 – 98. Retrieved from Directory

of Open AccessJournals.

Newcombe, T. (2016). Can security awareness training change behavior and reduce risk?

*Government Technology*. Retrieved from https://www.govtech.com/security/Can

Security Awareness-Training-Change-Behavior-and-Reduce-Risk.html

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T.

(2017). The human aspects of information security questionnaire (HAIS-Q): Two

further validation studies. *Computers & Security, 66*, 40-51. https://dx.doi.org/

10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). An

analysis of information security vulnerabilities at three Australian government

organizations. *Proceedings of the European Information Security Multi-Conference*

*(EISMC 2013).* Retrieved from https://pdfs.semanticscholar.org/fc19/b83fc28316

69d07e37131e1e8a4616b945a0.pdf

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014).

Determining employee awareness using the human aspects of information security

questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176. doi:10.1016/j.cose.

2013.12. 003

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing

information security awareness at an Australian bank: A comparative study.

*Information & Computer Security, 25*(2), 181-189. doi: 10.1108/ICS-03-2017-0017.

Petty, R., & Cacioppo, J. (1981). Attitudes and persuasion: Classic and contemporary

approaches. Dubuque, IA: W. M. C. Brown.

Pyzik, K. (2015). Shutting the door on social engineering. *Internal Auditor, 72*(5), 20 –

21. Retrieved from Business Source Premier.

Race and Ethnicity: The Science of Race. (n.d.). *Psychology Today*. Retrieved from

https://www.psychologytoday.com/us/basics/race-and-ethnicity

Ritzman, M. & Kahle-Piasecki, L. (2016). What works: A systems approach to employee

performance in strengthening information security. *Performance Improvement, 55*(8),

17 – 22. doi: 10.1002/pfi.21614

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change.

*The Journal of Psychology, 91*(1), 93-114. https://doi.org/10.1080/ 00223980.

1975.9915803

Salerno, J. & Peter-Hagene, L. (2015). One angry woman: Anger expression increases

influence for men, but decreases influence for women, during group deliberation. *Law*

*and Human* *Behavior, 39*(6), 581 – 592. doi: 10.1037/lhb0000147

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for

phish? A demographic analysis of phishing susceptibility and effectiveness of

interventions. In Proceedings of the SIGCHI Conference on Human Factors in

Computing Systems. SBA - Small Business Profile (2018). *U.S. Small Business*

*Administration Office of Advocacy.* Retrieved from https://www.sba.gov/sites/

default/files/advocacy/2018-Small-Business-Profiles-US.pdf

Smith, M. (2016). Social engineers reveal why the biggest threat to your business could

be you. Retrieved from https://www.theguardian.com/small-businessnetwork/

2016/oct/04/socialengineers-reveal-biggest-threat-business

Snyman, D. & Kruger, H. (2016). Behavioural thresholds in the context of information

security. *Proceedings of the Tenth International Symposium on Human Aspects of*

*Information* *Security & Assurance.* Retrieved from https://www.researchgate. net/

Publications/314838010\_Behavioural\_Thresholds\_in\_the\_Context\_of\_Information\_

Security

Social desirability bias. (2004). *The SAGE Encyclopedia of Social Science Research*

*Methods.* https://dx.doi.org/10.4135/9781412950589.n932

Stewart, H. & Jurjens, J. (2017). Information security management and the human

aspects in organizations. *Information & Computer Security, 25*(5), 494 – 534. doi:

10.1108/ICS-07-2016-0054

Tetri, P. & Vuorinen. (2013). Dissecting social engineering. *Behavior & Information*

*Technology, 32*(10). doi: 10.1080/0144929X.2013.763860

Uebelacker, S. & Quiel, S. (2014). The social engineering personality framework,

presented at the Workshop on Socio-Technical Aspects in Security and Trust, Vienna,

2014. doi:10.1109/stast.2014.12

United States Department of Labor. (2019). *Fair Labor Standards Act Advisor.* Retrieved

From https://webapps.dol.gov/elaws/faq/esa/flsa/014.htm

Van Bavel, R., Rodriguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection

motivation theory in the design of nudges to improve online security behavior.

*International Journal of* *Human* *Computer Studies, 123*, 29-39. https://doi.org/10.

1016/j.ijhcs.2018.11.003

Van Kleef, G., van den Berg, H., & Heerdink, M. (2015). The persuasive power of

emotions: Effects of emotional expressions on attitude formation and change.

*American Psychological Association, 100*(4), 1124 – 1142. http://dx.doi.org

/10.1037/apl0000003

Vishwanath, A., Harrison, B., & Ng, Y. (2016). Suspicion, cognition, and automaticity

model of phishing susceptibility. *Communication Research, 45*(8), 1-21. doi:

10.117/0093650215627483

Vishwanath, A., Herath, T., Chen, R., Wang, J., Rao, H. (2011). Why do people get

phished? Testing individual differences in phishing vulnerability within an integrated

information processing model. Decision Support Systems. 51(3), 576-586. doi:

10/1016/j.dss.2011.103002

Watering hole attacks – CompTIA Security + SY0-501-1.2 (2017). Retrieved from

https://www.professormesser.com/security-plus/sy0-501/watering-hole-attacks/

Williams, E., Hinds, J., & Joinson, A. (2018). Exploring susceptibility to phishing in the

workplace. *International Journal of Human-Computer Studies, 120*, 1-13.

https://doi.org/10.1016/j.ijhcs.2018.06.004

Workman, M. (2007). Gaining access with social engineering: An empirical study of the

threat. Information Systems *Security*. *16*, 315-331. doi: 10.1080/10658980701788165

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and

pretext social engineering threats to information security. *Journal of the American*

*Society for Information Science and Technology*. *59*(4), 662-674. DOI: 10.1002/

asi.20779

Wright, R., Chakraborty, S., Basoglu, K., & Marett, K. (2010). Where did they go right?

Understanding the deception in phishing communications. *Group Decision and*

*Negotiation, 19*(4), 391 – 416. doi: 10.1007/s10726-009-9167-9.

Unintentional insider threats: Social engineering. (2014). Software Engineering Institute,

Carnegie Melon University. Retrieved from https://resources.sei.cmu.edu/asset\_files/

TechnicalNote/2014\_004\_001\_77459.pdf

Young, W. & Leveson, N. (2014). Inside risks: An integrated approach to safety and

security based on systems theory. *Communications of the ACM, 57*(2). doi: 10.1145/

2556938

Zheng, Y., Robertson, T., Yan, R., Park, S., Bordoff, S., Chen, Q., & Sprissler, E. (2018).

Finding the weakest links in the weakest link: How well do undergraduate students

make cybersecurity judgment? *Computers in Human Behavior, 84*, 375-382.

https://doi.org/10.1016/j.chb2018.02 [019](https://doi.org/10.1016/j.chb.2018.02.019)

**Appendix A**

**Business Owner / Employee Recruitment Letter**

Dear Business Owner / Employee,

My name is Amy Washo, and I am a faculty member and doctoral student at Marywood University. I am conducting a research study. Its purpose is to obtain your opinions regarding information security awareness in the work place. I’ve been working towards my PhD for four years and your input into my final project would be so very much appreciated.

To qualify, participants in my study must be at least 18 years of age, a full-time or part-time employee of a small business in northeastern Pennsylvania that employs less than 25 people, and have a company email address. The research will take place through an online survey via REDCap. It will take about 15 – 20 minutes to complete.

Please know that this survey will not impact your business, either positively or negatively. Since it takes a relatively short amount of time to complete, it should not cause a disruption in any of your daily business activities.

Regarding the survey questions, I know there are ways that people would suggest are the right or wrong thing to do, but I want to know how you would honestly think, feel, or behave in each of these scenarios you are provided in the survey. It’s completely ok to think, feel, or behave in what some would consider the “wrong way.” I am looking for truthfulness and nothing more.

Completion of the survey is optional. All responses will be anonymous, confidential, and cannot be used to identify you.

**If you are eligible and willing to participate in this study, please click the link below to take the survey. Please also forward this email to your employees if you have any.**

https://redcap.marywood.edu/redcap/surveys/?s=L4MPCXHER8

Please don’t hesitate to contact me with any questions, or you may contact my dissertation advisor, Dr. Alan Levine, at levine@marywood.edu.

This study has been approved by Marywood University’s Exempt Review Committee.

**Appendix B**

**Informed Consent Form**

**Social Engineering Susceptibility: A Study on Demographics and Information Security Awareness in Small Businesses**

**Introduction**

You are invited to participate in a research study about information security awareness. You were chosen as a possible participant because you are 18 years of age or older, employed by a small business located in northeastern Pennsylvania, and have a company email address. Please read this form. Ask any questions you may have before agreeing to take part in this study.

This study is being conducted by a faculty member and doctoral candidate, Amy Washo, at Marywood University as part of a PhD dissertation.

**Purpose - What the Study is About**

The purpose of this study is to examine your opinions regarding information security awareness in the work place and then use your responses to determine susceptibility to social engineering. Social engineering can be defined as the use of psychological manipulation to gain access to confidential information.

**Procedures - What You Will Be Asked to Do**

If you agree to be in this study, you will be asked to complete a brief online survey via REDCap. This is a one-time survey that should take no more than 15-20 minutes of your time.

**Risks and Benefits**

The risk in this study is no greater than the risks experienced in daily life or activities.  
  
The benefits in this study are an increased understanding of the complexities of information security. This research may contribute to forming a model of information security best practices that can be of benefit to you and your company.

**Payment/Rewards**

No payment or reward will be given for participation in this survey.

**Confidentiality**

The records of this study will be kept private. Information used in any written or presented report will not make it possible to identify you. The main investigator and her three dissertation committee members will have access to the research records. The data obtained has the potential to be shared with other agencies and institutions, but this will not impact the confidentiality of the survey responses. Records will be kept for six months and then destroyed.

No computer transmission can be perfectly secure. However, reasonable efforts will be made to protect the confidentiality of your transmission.

**Taking Part is Voluntary**

Your participation is voluntary. Your decision to participate or not participate will not affect your current or future relations with the investigator. It will not affect your relations with Marywood University or your company. You may withdraw at any time without penalty or loss of benefits to which you are entitled. You may withdraw at any time up until the point you submit your survey by simply closing out of the internet browser. Since the survey results are anonymous to the investigator, once you complete the survey, your answers cannot be withdrawn.

**Contacts and Questions**

The interviewer conducting this study is Amy Washo.

You may ask questions now or later. If you have questions later, you may contact the researcher at awasho@maryu.marywood.edu or 570-348-6274. If you prefer, you may also contact Dr. Alan Levine, Professor at Marywood University and dissertation chair, at levine@marywood.edu or 570-348-6290.

If you have questions related to the rights of research participants, please contact Ms. Courene M. Loftus, MPA, CIP, Marywood University’s Director of Human Participants Protection and Research Compliance, at (570) 961-4782 or cloftus@marywood.edu.

You may print a copy of this form to keep for your records.

**Statement of Consent**

By proceeding with this survey, I acknowledge that I have read and understood this form. I consent to participate in this study.

**Appendix C**

**Human Aspects of Information Security Questionnaire**

|  | Strongly Disagree | Disagree | Neither Agree nor Disagree | Agree | Strongly Agree |
| --- | --- | --- | --- | --- | --- |
| **Knowledge** |  |  |  |  |  |
| It is acceptable to use my social media passwords on my work accounts. |
| I am allowed to share my work passwords with colleagues. |
| A mixture of letters, numbers, and symbols is necessary for work passwords. |
| I am allowed to click on any links in emails from people I know. |
| I am not permitted to click on a link in an email from an unknown sender. |
| I am allowed to open email attachments from unknown senders. |
| I am allowed to download any files onto my work computer if they help me to do my job. |
| While I am at work, I shouldn’t access certain websites. |
| I am allowed to enter any information on any website if it helps me do my job. |
| When working in a public place, I have to keep my laptop with me at all times. |
| I am allowed to send sensitive work files via a public wi-fi network. |
| When working on a sensitive document, I must ensure that strangers can’t see my laptop screen. |
| Sensitive print-outs can be disposed of in the same way as non-sensitive ones. |
| If I find a USB stick in a public place, I shouldn’t plug it into my work computer. |
| I am allowed to leave print-outs containing sensitive information on my desk overnight. |
| **Attitude** |  |  |  |  |  |
| It is safe to use the same passwords for social media and work accounts. |
| It’s a bad idea to share my work passwords, even if a colleague asks for it. |
| It’s safe to have a work password with just letters. |
| It’s always safe to click on links in emails from people I know. |
| Nothing bad can happen if I click on a link in an email from an unknown sender. |
| It’s risky to open an email attachment from an unknown sender. |
| It can be risky to download files on my work computer. |
| Just because I can access a website at work, doesn’t mean that it’s safe. |
| If it helps me to do my job, it doesn’t matter what information I put on a website. |
| When working in a café, it’s safe to leave my laptop unattended for a minute. |
| It’s risky to send sensitive work files using a public wi-fi network. |
| Disposing of sensitive print-outs by putting them in trash bins is safe. |
| If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer. |
| It’s risky to leave print-outs that contain sensitive information on my desk overnight. |
| **Behavior** |  |  |  |  |  |
| I use different passwords for social media and work accounts. |
| I share my work passwords with colleagues. |
| I use a combination of letters, numbers, and symbols in my work passwords. |
| I don’t always click on links in emails just because they come from someone I know. |
| If an email from an unknown sender looks interesting, I click on a link within it. |
| I don’t open email attachments if a sender is unknown to me. |
| I download any files onto my work computer that will help me get the job done. |
| When accessing the internet at work, I visit any website that I want to. |
| I assess the safety of websites before entering information. |
| When working in a public space, I leave my laptop unattended. |
| I send sensitive work files using a public wi-fi network. |
| I check that strangers can’t see my laptop screen if I’m working on a sensitive document. |
| When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed. |
| I wouldn’t plug a USB stick found in a public place into my work computer. |
| I leave print-outs that contain sensitive information on my desk when I’m not there. |  |  |  |  |  |

**Appendix D**

**Demographic Survey Questions**

1. Do you work for a small business in Northeastern Pennsylvania that employs less than 25 people?

Yes No

1. Do you have a company email address?

Yes No

1. What is your gender?

Male

Female

Other

Prefer Not to Answer

1. What is your age? \_\_\_\_\_\_\_\_\_
2. What is the highest level of education you have received?

Less Than High School

High School Diploma

Associate’s Degree

Bachelor’s Degree

Master’s Degree

Terminal Degree

1. How long have you worked for your current company?

Less than 1 year

1 – 3 years

4 – 6 years

7 – 9 years

10 or more years

1. What is the average number of hours per week that you work? \_\_\_\_\_\_\_\_
2. In what industry do you work?

Healthcare

Marketing

Construction

Technology

Nonprofit

Law

Finance

Insurance

Other

1. Thinking about the last three years, how many times per year on average have you received training or education on cyber security awareness?

0

1 time

2 times

3 times

More than 3 times

1. What is your rank in the company?

Owner / Highest Ranking Official

Non-Owner / Non-Highest Ranking Official

1. Which of the following represents the cultural identity with which you most identify?

American

Latino

Asian

Indian

Canadian

British / European

Middle Eastern

African

Other

**Appendix E**

*Participants’ Age*

| Age | Frequency | Percent |
| --- | --- | --- |
| 19 | 1 | 1.1 |
| 22 | 2 | 2.1 |
| 23 | 1 | 1.1 |
| 24 | 1 | 1.1 |
| 25 | 4 | 4.2 |
| 27 | 2 | 2.1 |
| 28 | 3 | 3.2 |
| 29 | 2 | 2.1 |
| 30 | 2 | 2.1 |
| 31 | 2 | 2.1 |
| 32 | 1 | 1.1 |
| 33 | 2 | 2.1 |
| 34 | 4 | 4.2 |
| 35 | 1 | 1.1 |
| 36 | 3 | 3.2 |
| 37 | 3 | 3.2 |
| 38 | 5 | 5.3 |
| 39 | 4 | 4.2 |
| 40 | 2 | 2.1 |
| 41 | 2 | 2.1 |
| 42 | 2 | 2.1 |
| 43 | 2 | 2.1 |
| 44 | 2 | 2.1 |
| 45 | 1 | 1.1 |
| 46 | 1 | 1.1 |
| 47 | 3 | 3.2 |
| 48 | 2 | 2.1 |
| 49 | 5 | 5.3 |
| 50 | 3 | 3.2 |
| 51 | 3 | 3.2 |
| 52 | 3 | 3.2 |
| 53 | 1 | 1.1 |
| 54 | 3 | 3.2 |
| 55 | 2 | 2.1 |
| 56 | 1 | 1.1 |
| 57 | 2 | 2.1 |
| 59 | 1 | 1.1 |
| 60 | 2 | 2.1 |
| 64 | 2 | 2.1 |
| 67 | 2 | 2.1 |
| 69 | 1 | 1.1 |
| 70 | 1 | 1.1 |
| 75 | 1 | 1.1 |

**Appendix F**

**Knowledge Score**

*Participants’ Knowledge Score*

| Knowledge Score | Frequency | Percent |
| --- | --- | --- |
| 35 | 1 | 1.1 |
| 36 | 2 | 2.2 |
| 39 | 1 | 1.1 |
| 43 | 1 | 1.1 |
| 44 | 1 | 1.1 |
| 45 | 2 | 2.1 |
| 46 | 1 | 1.1 |
| 47 | 1 | 1.1 |
| 48 | 1 | 1.1 |
| 49 | 3 | 3.2 |
| 50 | 4 | 4.2 |
| 51 | 2 | 2.1 |
| 52 | 4 | 4.2 |
| 53 | 5 | 5.3 |
| 54 | 2 | 2.1 |
| 55 | 3 | 3.2 |
| 56 | 3 | 3.2 |
| 57 | 5 | 5.3 |
| 58 | 6 | 6.3 |
| 59 | 4 | 4.2 |
| 60 | 3 | 3.2 |
| 61 | 2 | 2.1 |
| 62 | 5 | 5.3 |
| 63 | 6 | 6.3 |
| 64 | 3 | 3.2 |
| 65 | 1 | 1.1 |
| 66 | 2 | 2.1 |
| 67 | 3 | 3.2 |
| 68 | 3 | 3.2 |
| 69 | 1 | 1.1 |
| 70 | 2 | 2.1 |
| 71 | 2 | 2.1 |
| 72 | 2 | 2.1 |
| 73 | 2 | 2.1 |
| 74 | 2 | 2.1 |
| 75 | 4 | 4.2 |

*Participants’ Attitude Score*

|  |  |  |
| --- | --- | --- |
| Attitude Score | Frequency | Percent |
| 39 | 1 | 1.1 |
| 46 | 2 | 2.1 |
| 52 | 1 | 1.1 |
| 54 | 4 | 4.2 |
| 55 | 1 | 1.1 |
| 56 | 1 | 1.1 |
| 58 | 4 | 4.2 |
| 59 | 5 | 5.3 |
| 60 | 6 | 6.3 |
| 61 | 4 | 4.2 |
| 62 | 5 | 5.3 |
| 63 | 6 | 6.3 |
| 64 | 2 | 2.1 |
| 65 | 8 | 8.4 |
| 66 | 2 | 2.1 |
| 67 | 7 | 7.4 |
| 68 | 2 | 2.1 |
| 69 | 4 | 4.2 |
| 70 | 4 | 4.2 |
| 71 | 6 | 6.3 |
| 72 | 4 | 4.2 |
| 73 | 3 | 3.2 |
| 74 | 3 | 3.2 |
| 75 | 10 | 10.5 |

*Participants’ Behavior Score*

|  |  |  |
| --- | --- | --- |
| Behavior Score | Frequency | Percent |
| 36 | 1 | 1.1 |
| 43 | 1 | 1.1 |
| 46 | 1 | 1.1 |
| 48 | 2 | 2.1 |
| 49 | 1 | 1.1 |
| 51 | 2 | 2.1 |
| 52 | 1 | 1.1 |
| 54 | 1 | 1.1 |
| 55 | 5 | 5.3 |
| 56 | 6 | 6.3 |
| 57 | 4 | 4.2 |
| 58 | 6 | 6.3 |
| 59 | 3 | 3.2 |
| 60 | 4 | 4.2 |
| 61 | 3 | 3.2 |
| 62 | 3 | 3.2 |
| 63 | 7 | 7.4 |
| 64 | 4 | 4.2 |
| 65 | 7 | 7.4 |
| 66 | 4 | 4.2 |
| 67 | 2 | 2.1 |
| 68 | 4 | 4.2 |
| 69 | 3 | 3.2 |
| 70 | 4 | 4.2 |
| 71 | 7 | 7.4 |
| 72 | 2 | 2.1 |
| 73 | 3 | 3.2 |
| 74 | 1 | 1.1 |
| 75 | 3 | 3.2 |

**Appendix G**

**Information Security Awareness (ISA) Score & Susceptibility Score**

*Participants’ ISA Score*

| ISA Score | Frequency | Percent |
| --- | --- | --- |
| 118 | 1 | 1.1 |
| 138 | 1 | 1.1 |
| 141 | 1 | 1.1 |
| 143 | 1 | 1.1 |
| 144 | 1 | 1.1 |
| 148 | 1 | 1.1 |
| 151 | 1 | 1.1 |
| 159 | 1 | 1.1 |
| 161 | 1 | 1.1 |
| 163 | 2 | 2.1 |
| 164 | 2 | 2.1 |
| 165 | 3 | 3.2 |
| 166 | 1 | 1.1 |
| 167 | 1 | 1.1 |
| 168 | 2 | 2.1 |
| 169 | 1 | 1.1 |
| 170 | 4 | 4.2 |
| 171 | 1 | 1.1 |
| 172 | 2 | 2.1 |
| 173 | 1 | 1.1 |
| 174 | 2 | 2.1 |
| 175 | 2 | 2.1 |
| 176 | 1 | 1.1 |
| 178 | 2 | 2.1 |
| 179 | 1 | 1.1 |
| 180 | 2 | 2.1 |
| 181 | 4 | 4.2 |
| 184 | 2 | 2.1 |
| 185 | 1 | 1.1 |
| 186 | 2 | 2.1 |
| 187 | 1 | 1.1 |
| 189 | 1 | 1.1 |
| 190 | 3 | 3.2 |
| 191 | 1 | 1.1 |
| 192 | 2 | 2.1 |
| 193 | 2 | 2.1 |
| 194 | 3 | 3.2  195 |
| 195 | 1 | 1.1 |
| 196 | 1 | 1.1 |
| 197 | 1 | 1.1 |
| 198 | 2 | 2.1 |
| 199 | 2 | 2.1 |
| 200 | 1 | 1.1 |
| 201 | 4 | 4.2 |
| 203 | 1 | 1.1 |
| 206 | 1 | 1.1 |
| 207 | 2 | 2.1 |
| 209 | 1 | 1.1 |
| 211 | 2 | 2.1 |
| 212 | 3 | 3.2 |
| 213 | 1 | 1.1 |
| 214 | 2 | 2.1 |
| 215 | 1 | 1.1 |
| 216 | 2 | 2.1 |
| 220 | 2 | 2.1 |
| 221 | 1 | 1.1 |
| 224 | 2 | 2.1 |
| 225 | 1 | 1.1 |

*Participants’ Susceptibility Score*

| Susceptibility Score | Frequency | Percent |
| --- | --- | --- |
| .00 | 1 | 1.1 |
| .56 | 2 | 2.1 |
| 2.22 | 1 | 1.1 |
| 2.78 | 2 | 2.1 |
| 5.00 | 2 | 2.1 |
| 5.56 | 1 | 1.1 |
| 6.11 | 2 | 2.1 |
| 6.67 | 1 | 1.1 |
| 7.22 | 3 | 3.2 |
| 7.78 | 2 | 2.1 |
| 8.89 | 1 | 1.1 |
| 10.00 | 2 | 2.1 |
| 10.56 | 1 | 1.1 |
| 12.22 | 1 | 1.1 |
| 13.33 | 4 | 4.2 |
| 13.89 | 1 | 1.1 |
| 14.44 | 2 | 2.1 |
| 15.00 | 2 | 2.1 |
| 15.56 | 1 | 1.1 |
| 16.11 | 1 | 1.1 |
| 16.67 | 1 | 1.1 |
| 17.22 | 3 | 3.2 |
| 17.78 | 2 | 2.1 |
| 18.33 | 2 | 2.1 |
| 18.89 | 1 | 1.1 |
| 19.44 | 3 | 3.2 |
| 20.00 | 1 | 1.1 |
| 21.11 | 1 | 1.1 |
| 21.67 | 2 | 2.1 |
| 22.22 | 1 | 1.1 |
| 22.78 | 2 | 2.1 |
| 24.44 | 4 | 4.2 |
| 25.00 | 2 | 2.1 |
| 25.56 | 1 | 1.1 |
| 26.11 | 2 | 2.1 |
| 27.22 | 1 | 1.1 |
| 27.78 | 2 | 2.1 |
| 28.33 | 2 | 2.1 |
| 28.89 | 1 | 1.1 |
| 29.44 | 2 | 2.1 |
| 30.00 | 1 | 1.1 |
| 30.56 | 4 | 4.2 |
| 31.11 | 1 | 1.1 |
| 31.67 | 2 | 2.1 |
| 32.22 | 1 | 1.1 |
| 32.78 | 1 | 1.1 |
| 33.33 | 3 | 3.2 |
| 33.89 | 2 | 2.1 |
| 34.44 | 2 | 2.1 |
| 35.56 | 1 | 1.1 |
| 36.67 | 1 | 1.1 |
| 41.11 | 1 | 1.1 |
| 42.78 | 1 | 1.1 |
| 45.00 | 1 | 1.1 |
| 45.56 | 1 | 1.1 |
| 46.67 | 1 | 1.1 |
| 48.33 | 1 | 1.1 |
| 59.44 | 1 | 1.1 |

**Appendix H**

*Knowledge Score - Mean and Standard Deviations for Industries*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *n* | Mean Knowledge Score | Standard Deviation |
| Healthcare | 4 | 60 | 11.52 |
| Marketing | 3 | 54 | 4.36 |
| Construction | 4 | 64 | 8.6 |
| Technology | 27 | 58.96 | 9.84 |
| Nonprofit | 11 | 57.64 | 7.17 |
| Law | 3 | 60.33 | 14.57 |
| Finance | 5 | 54 | 6.2 |
| Insurance | 1 | 64 | - |
| Other | 37 | 58.65 | 10.03 |

*Attitude Score - Mean and Standard Deviations for Industries*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *n* | Mean Attitude Score | Standard Deviation |
| Healthcare | 4 | 67.75 | 8.38 |
| Marketing | 3 | 62.67 | 4.04 |
| Construction | 4 | 68.75 | 4.03 |
| Technology | 27 | 65.63 | 6.22 |
| Nonprofit | 11 | 65.18 | 6.43 |
| Law | 3 | 67 | 8 |
| Finance | 5 | 65.8 | 5.93 |
| Insurance | 1 | 75 | - |
| Other | 37 | 63.43 | 8.58 |

*Behavior Score - Mean and Standard Deviations for Industries*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *n* | Mean Behavior Score | Standard Deviation |
| Healthcare | 4 | 61.25 | 7.41 |
| Marketing | 3 | 56.67 | 9.02 |
| Construction | 4 | 66.75 | 3.86 |
| Technology | 27 | 62 | 7.12 |
| Nonprofit | 11 | 64.27 | 6.18 |
| Law | 3 | 66 | 7.94 |
| Finance | 5 | 56.8 | 2.95 |
| Insurance | 1 | 73 | - |
| Other | 37 | 8.69 | 1.43 |

*Susceptibility Score - Mean and Standard Deviations for Industries*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *n* | Mean Susceptibility Score | Standard Deviation |
| Healthcare | 4 | 20 | 14.83 |
| Marketing | 3 | 28.7 | 6.86 |
| Construction | 4 | 14.17 | 7.57 |
| Technology | 27 | 21.34 | 11.2 |
| Nonprofit | 11 | 21.06 | 9.63 |
| Law | 3 | 17.59 | 16.68 |
| Finance | 5 | 26.89 | 7.39 |
| Insurance | 1 | 7.22 | - |
| Other | 37 | 22.63 | 14.17 |