5-2021

A Framework to Detect the Susceptibility of Employees to Social Engineering Attacks

Hashim H. Alneami
alneamih@my.erau.edu

A FRAMEWORK TO DETECT THE SUSCEPTIBILITY OF EMPLOYEES TO SOCIAL ENGINEERING ATTACKS

by

Hashim H. Alneami

A thesis submitted in partial fulfillment of the requirements for the degree of

Master of Science in Cybersecurity Engineering

at Embry-Riddle Aeronautical University

Department of Electrical Engineering and Computer Science

Embry-Riddle Aeronautical University

Daytona Beach, Florida

May 2021

A FRAMEWORK TO DETECT THE SUSCEPTIBILITY OF EMPLOYEES TO SOCIAL ENGINEERING ATTACKS

by Hashim H. Alneami

This thesis was prepared under the direction of the candidate's Thesis Committee Chair, Dr. Laxima Niure Kandel, and has been approved by the members of the thesis committee. It was submitted to the Department of Electrical Engineering and Computer Science in partial fulfillment of the requirements for the Degree of Master of Science in Cybersecurity Engineering.

_____
Laxima Niure Kandel, Ph.D.
Committee Chair

_____
Houbing Song, Ph.D.
Committee Member

_____
Richard S. Stansbury, Ph.D.
Committee Member

_____ _____
Timothy A. Wilson, Sc.D. Date
Chair, Electrical Engineering and Computer Science

_____ _____
Maj Mirmirani, Ph.D. Date
Dean, College of Engineering

_____ _____
Christopher Grant, Ph.D. Date
Associate Provost of Academic Support

Acknowledgments

Thank you to my loving parents and family for the unconditional love and support. You will always come first. I would also like to thank my supervisor, Dr. Laxima Niure Kandel, for providing guidance and feedback throughout this project. My gratitude extends to the respectful committee members, and all the faculty members with whom I had the pleasure to work with.

Table of Contents

List of Tables

List of Figures

Abstract

Social engineering attacks (SE-attacks) in enterprises are hastily growing and are becoming increasingly sophisticated. Generally, SE-attacks involve the psychological manipulation of employees into revealing confidential and valuable company data to cybercriminals. The ramifications could bring devastating financial and irreparable reputation loss to the companies. Because SE-attacks involve a human element, preventing these attacks can be tricky and challenging and has become a topic of interest for many researchers and security experts. While methods exist for detecting SE-attacks, our literature review of existing methods identified many crucial factors such as the national cultural, organizational, and personality traits of employees that enable SE-attacks not considered by the other researchers. Thus, this thesis aims to address the gap by identifying and analyzing all the factors that make the SE-attack possible. We have developed a framework that operates in an enterprise environment and can detect the susceptibility of victims to SE-attacks. It relies on mapping Gragg's psychological triggers of social engineering to three groups of factors, namely the national cultural factors, the organizational factors, and the personality traits of employees. Our analysis demonstrates that there is a correlation between the social engineering triggers and the three-layered factors that make employees susceptible to social engineering attacks. Thus, adding these factors in the proposed framework detects susceptibility of victims. Finally, we introduce a proposed framework that would detect and recognize weaknesses and susceptibility of employees in an organization which can be used for enhancing awareness and employee training to better recognize and prevent SE-attacks.

Chapter 1: Introduction

1.1 Theoretical Background

Over the past years, social engineering attacks have proven to be one of the biggest concerns affecting the IT infrastructure, both in the private and public sectors. The damage it has imposed on corporates and the difficulty of avoiding such attacks have made social engineering the center point for many security experts and researchers. One issue that has been discussed immensely regarding social engineering is the human factor and its impact on the recurring success of these attacks. It has become widely known for many scholars that the human element is the weakest link in any IT system (Mitnick, Simon, & L., 2003) and (GBC-DELL Survey, 2015). How employees think and behave in the workplace is considered an important factor that can lead to more or less amounts of cyber threats (Ranjeev & Lawless, 2015). Therefore, it is crucial to study the factors and reasons influencing the behavior and values of employees to have a better understanding of how to deal with human-based attacks such as social engineering attacks.

To understand the issue more clearly, we must first understand what we mean by social engineering attacks and how they are carried out. One definition states that social engineering is the use of psychological influence to manipulate a victim and gain his trust so he would be eventually revealing information (Allen, 2006, p.4). From that definition, we discover that the potential success of these attacks relies mainly on the vulnerability of the human factor. According to Ross (Ross, 2006), systems consist of three elements: hardware, software, and wetware. Wetware represents the human element in the system. Regardless of the amount of money and work put into enforcing the security of the IT infrastructure, a social engineer can patiently exploit the weaknesses of human nature and gain unauthorized access to sensitive information using his knowledge of psychological tricks and triggers (Allen, 2006, p.4).

There are several factors on different levels that can influence the target and play a role in defining the possibility of the success of social engineering attacks. Some of the factors are related to the personality features of the victims and how they behave socially. Others are concerned with cultural factors designed by the society people live in. These factors play a role in social engineering attacks and can be used to measure the susceptibility of individuals based on them.

Based on previous research, there has been some work done towards mapping the psychological triggers of SE attacks to human-based factors. One of the studies focused on mapping Cialdini's principles of persuasion to the five personality traits of a victim (Uebelacker, S., & Quiel, S. 2014). However, there has not been a framework designed to take into consideration the impact of other factors that can be influenced by the environment of the victims. Even though researchers have indicated the existence of a relationship between the susceptibility of SE attacks and various factors (Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F., 2009), we believe a framework that can map that

relationship is needed to be designed as it can provide a better understanding of the SE attacks and how can we come up with more successful countermeasures. Cultural factors are some of these influencers that can dictate humans' mentality and behavior. These factors can be defined on a national scale or within the organization, which can be perceived as national and corporate culture. Their importance comes from their role in defining the environment of the employees that can be targeted, and analyzing such factors will give us a broader view of social engineering attacks enabling causes.

Expanding the cultural vision from corporate to national can provide us with a better idea of how culture in general influences and affects security-related issues (Übelacker, S., 2013). Moreover, as national cultures exist on a higher layer, they are excluded from an organization's influence which makes them offer a cultural frame in which organizational cultures thrive (Übelacker, S., 2013). In addition, behaviors related to national cultures must be considered when we study and evaluate organizational cultures (Übelacker, S., 2013).

Based on our evaluation of existing research on the topic, we have developed a framework that is used to detect the susceptibility of social engineering attacks of victims. The framework focuses on the victims operating mainly in an organizational environment. It relies on mapping Gragg's psychological triggers of social engineering to three groups of factors. These groups are the national cultural factors, the organizational factors, and the occupational personality traits. By covering these three groups of factors, we would have a layered and comprehensive approach that can enable us to analyze and detect the possible reasons that can lead to SE attacks in any given environment. Also, we also provided an additional framework that can use the result of the factors' impact in measuring the susceptibility of workers in certain organization, and creating a tailored awareness program. We firmly believe that such a framework will manage to cover the main factors that can influence victims in any given organization.

In the next sections, we will start by defining the concept of social engineering. Then, we are going to discuss the components of our suggested framework that measures the impact of the factors, and define their elements. We describe the psychological triggers of SE created by Gragg. Then, we will define the three groups of factors and what each factor represents. Finally, we are going to define our framework and discuss the mapped relationships between the factors and the triggers. Finally, we introduce a proposed framework that would detect and recognize weaknesses and susceptibility of employees in an organization, and would provide the ability to design a personalized training and education program to raise employee's awareness against cybersecurity threats.

1.2. Social Engineering Definitions

1.2.1 In Social Science

Within the context of social science, Social Engineering is defined as the discipline that focuses on manipulating and influencing people's popular beliefs, attitudes, actions, and social behaviors at a wide level (Stergiou, D., 2013). In Wikipedia, social engineering is

defined as a top-down process used to influence specific behaviors and social attitudes on a high level for the purpose of producing sought characteristics in a target or a group of targets (Wikipedia, 2021).

1.2.2 In Information Security

Researchers have profoundly covered the definition of social engineering within the context of information security. According to (Mann, M. I., 2012), social engineering is the art of manipulating people using deception for the sake of obtaining information from them or persuade them to perform an action. Hadnagy (2010) elaborated furthermore to state that the solicited action may or may not in the deceived people's interest. Although according to Hadnagy (2010), that may be true when social engineering is applied to a field like medicine, it is inconceivable to presume common interest from social engineering in information security. Another definition states that social engineering is psychological exploitation that scammers utilize to manipulate human vulnerabilities and launch emotional-based attacks on vulnerable people (Atkins, 2013). One popular definition defines it as the act of manipulating a person to achieve objectives that may or may not be in the target's interests (Hadnagy et al., 2010).

Additionally, we found out that most of the researchers that studied social engineering shared the same fundamental idea, which revolves around exploiting the vulnerability of the human user (Mann, M. I., 2012) (Hadnagy, 2010) (Pfleeger, C. P., & Pfleeger, S., 2006) (Salahdine, F., & Kaabouch, N., 2019).

1.3 Psychological Triggers of Social Engineering

It is only logical to try to comprehend the psychology behind social engineering before developing a defense mechanism against it since it is both a social and psychological exercise (Gragg, (2003). In his work, (Gragg, 2003) has defined the psychological triggers which have the ability to influence or persuade people within the context of social engineering. He came up with seven triggers that are believed to be used by hackers and social engineers to manipulate their targets psychologically (Gragg, 2003). These triggers are shown in figure 1, and we will explain each trigger subsequently.

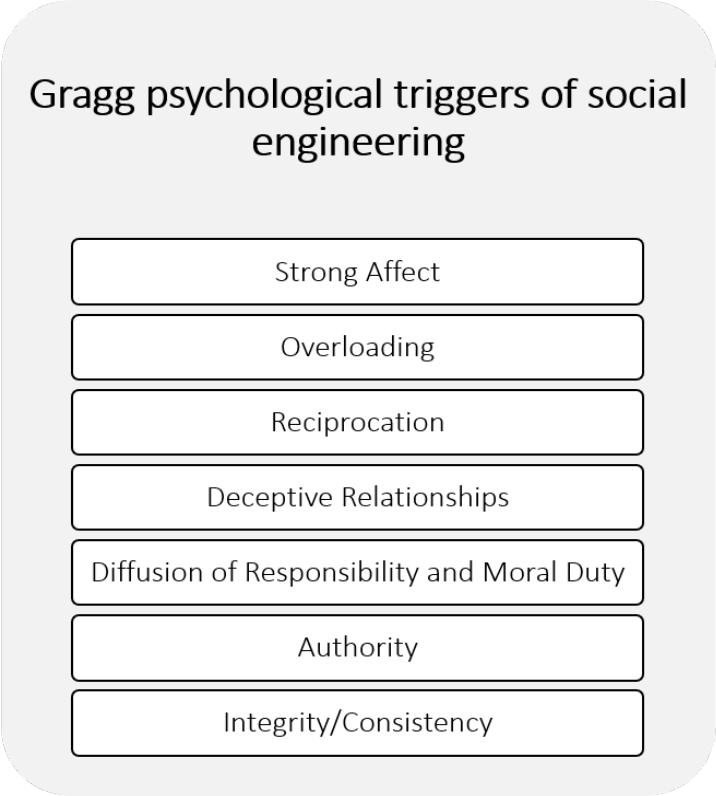

Figure 1 Psychological Triggers of Social Engineering

1.3.1 Strong Affect

Strong affect is a trigger that makes use of an intensified and heightened emotional state to allow a social engineer to obtain more than what would be reasonable (Gragg, 2003). To illustrate more, the victim is less likely to properly process presented arguments if he is experiencing a high sense of anger, surprise, or anticipation. Upon using this trigger, the hacker will trigger the targeted emotion to distract the victim and disturb their ability to think logically, evaluate, or create counterarguments (Scheeres, J. W., 2008).

1.3.2 Overloading

By implementing overloading, mistaken premises will be challenged as they are introduced hastily and are shoved between convincing arguments (Gragg, 2003). The victim's logical functioning will be affected if he must deal with a lot of information quickly which could lead to a state of overload. People become mentally passive when facing big amounts of information to process; they tend to accept information instead of evaluating it (Burtner, p. 2).

1.3.3 Reciprocation

It is commonly known as a rule in our daily social interactions that we should always return the favor of other people. People would return the favor even it is more valuable

than the original act, or the original act was not requested in the first place (Rusch, J. J., 1999). Reciprocation is regularly used in the corporate environment. Employees help each other out with the hope that the favor will be returned. It has become an unspoken system that is perceived crucial for the future success of the employees. Unfortunately, social engineers take advantage of this system (Gragg, 2003).

1.3.4 Deceptive Relationships

Deceptive relationships trigger is the concept of establishing a relationship with the aim of exploiting the other person (Gragg, 2003). It can be done in several ways, like sharing information or sharing a common enemy. There are many ways to exploit the relationship once it has been developed (Vigilante).

1.3.5 Diffusion of Responsibility and Moral Duty

This is a method where the hacker tricks the target into believing that they will be spared from responsibilities towards their actions, or their actions will hold a positive outcome (Scheeres, J. W., 2008). The targets are made to believe that their decisions will be the difference between the success or failure of the discussed situation (Gragg, 2003).

1.3.6 Authority

We normally respond to authority as it is in our human nature. Convincing the target that he is dealing with some authority figure can bring a great benefit for the social engineer. The fact that it is even more difficult to verify the authority of the perpetrator makes this a trigger a very powerful one (Gragg, 2003). In real life, we see this trigger being used widely by hackers.

1.3.7 Integrity/Consistency

In this trigger, the hackers will make use of people's inclination towards following commitments for the purpose of persuading them to execute some action (Gragg, 2003) (Scheeres, J. W. (2008)). From another aspect, "people have a tendency to believe that others are expressing their true attitudes when they make a statement" (Gragg, 2003). The tendency to believe others is based mainly on their own honesty in expressing emotions (Rusch, 1999).

1.4 National Cultures

In his 5-D model, Hofstede (1980) explained the five cultural dimensions per country. He defined them to include: power distance, individualism, masculinity, uncertainty avoidance, and long-term orientation (Hofstede Center.). It is considered that various nations react differently to anthropological issues. Those issues can include analyzing how to work out unfairness, behavior with regard to the relationship of individual in a community, how to handle uncertainty, and the assumptions of gender (Anon, 2015). According to available research, there is a need for more evaluation on the impact of these dimensions on security-related issues. Table 1 describes those five dimensions.

Table 1 Hofstede 5-D Model of National Culture. From (Hofstede Center) & (Übelacker, S., 2013).

Dimension	Description
Power Distance (PDI)	The expectation and acceptance of unequally distributed power among members of institutions and organizations in a country.
Individualism vs. Collectivism (IDV)	Reflects "the degree of interdependence a society maintains among its members."
Masculinity vs. Femininity (MAS)	Describes the motivation of people what they think is important to achieve. Wanting to be the best is "masculine"; liking what you do defined as "feminine".
Uncertainty Avoidance (UAI)	Specifies whether members of a culture experience "ambiguous or unknown situations" as a threat that needs to be avoided.
Long-Term vs. Short-Term Orientation (LTO)	Pictures the degree a society has towards a future-oriented or short-term perspective.

1.5 Organizational Cultures

According to (Hofstede Center.), "organizational culture is the way in which members of an organization relate to each other, their work and the outside world in comparison to other organizations". Organizational culture involves working people in an organization inducing on them a form of organizational behavior (Deal and Kennedy, 1982), (Scholz, 1987), (Watkins, 2013), and (A. Leroch, 2014). There have been many studies conducted on the topic of organizational culture. One of the studies is the Multi-Focus Model on Organizational Culture developed by Hofstede (Hofstede Center.). It concluded that there are six dimensions of organizational culture that can be used to measure the cultural level of a certain organization (Hofstede Center.). As shown in Table 2, These dimensions include organizational effectiveness, customer orientation, level of control, focus, approachability, and management philosophy.

Table 2 Hofstede Multi-Focus Model on Organizational Culture. From (Hofstede Center.)

Dimension	Description
Organizational effectiveness Means-Oriented VS. Goal-Oriented	• This dimension is closely connected to the effectiveness of the organization. • In a means-oriented culture, the key feature is the way in which work must be carried out, the "how". • In a goal-oriented culture, employees are primarily out to achieve specific internal goals or results, the "what".
Customer orientation Internally Driven VS. Externally Driven	• In a highly internally driven culture, employees perceive their task towards the outside world as a given, based on the idea that business ethics and honesty matter most. • In a very externally driven culture, the only emphasis is on meeting the customer's requirements; results are most important.
Level of control Easygoing Work Discipline VS. Strict Work Discipline	• This dimension refers to the amount of internal structuring, control, and discipline. • A very easygoing culture reveals an internal fluid structure, a lack of predictability, and little control and discipline. • A very strict work discipline reveals the reverse.
Focus Local VS. Professional	• In a local company, employees identify with the boss and/or the unit in which one works.

	• In a professional organization, the identity of an employee is determined by his profession and/or the content of the job.
Approachability Open System VS. Closed System	• This dimension relates to the accessibility of an organization. • In a very open culture, newcomers are made immediately welcome. • In a very closed organization, it is the reverse.
Management philosophy Employee-Oriented VS. Work-Oriented	• In very employee-oriented organizations, members of staff feel that personal problems are considered. • In very work-oriented organizations, there is heavy pressure to perform the task even if this is at the expense of employees.

1.6 Occupational Personality Traits

In previous studies, researchers have been studying the personality traits of employees within the work environment. Occupational grouping of personalities of workers can help to assess the organizational subcultures of the organization (Übelacker, 2013). Hossiep and Paschen (2012) developed their version of an employee's personality traits which is based on the employee's type of occupation. They named it "*Bochumer Inventar zur berufsbezogenen Persönlichkeits-beschreibung (BIP)";* it means a German personality inventory for organizational applications. The traits are comprised of occupational orientation, work behavior, interpersonal skills "social skills", and mental constitution.

Table 3 A German personality Inventory for Organizational Applications (Hossiep and Paschen, 2012).

Trait	Description
Occupational orientation	• It refers to the employee's motivation to work with a high standard of quality as well as the tendency to design processes and structures to use, and his motivation for social influence.
Work behavior	• It refers to the employee's level of conscientiousness, flexibility, and willingness to turn decisions into implementable activities.
Interpersonal skills (social skills)	• These skills include sensitivity, contacting ability, sociability, teamwork orientation, and assertiveness.
Mental constitution	• It defines an employee's emotional stability, resilience, and confidence.

After providing a theoretical background of the topic, we are going to present the thesis as follows: chapter 2 is going to discuss the suggested framework and the impact of its layers on the susceptibility of SE attacks as well as providing a statistical approach to find the significance. In chapter 3, the thesis will explain how to apply the framework practically. In chapter 4, we are going to provide our conclusion and the direction of future work.

Chapter 2: The Three-Layered Framework

2.1 Research Methodology

In this thesis, we adopted a theoretical approach to evaluate the correlation between the three-layered factors we used and the SE psychological triggers. We hope to validate the framework in the future by conducting empirical research to test our findings.

The examined studies show some shortcomings that an organization may encounter when implementing policies, countermeasures, and mechanisms for preventing social engineering attacks. For a start, a limitation in executing countermeasures originates from

the education, capability, skills, and personality traits of employees (Flores, & Ekstedt, 2013), (Peltier, 2006), and (Algarni et al., 2013).

The distinctions between workers create a significant challenge in the implementation process of defensive measures. Moreover, the difference in training and level of awareness amongst workers restricts the progress of these countermeasures as well (Fan, Lwakatare, & Rong, 2017), and (Mataracioglu, & Ozkan, 2011).

The methods used by attackers to obtain corporate sensitive information are always evolving. Protecting important information is reliant on the capability to influence and convince workers to adjust their behaviors and practices that lead to the disclosure of private information that can be used by attackers (Smith, Papadaki, & Furnell, 2013), and (Greavu-Serban, & Serban, 2014). Based on that, there is a need to address the role and impact of factors influencing the behavior of employees within an organization. We think that our framework will provide a mechanism to study such a phenomenon in the context of cultural influence.

We mainly focused on the impact of national cultural factors, organizational factors, and employees' personality traits on the susceptibility to SE attacks. It is based on our firm belief that the characteristics of the environment surrounding the targets in organizations can help increase or decrease their susceptibility to SE attacks. Therefore, we sought out the answers to the following questions:

- What are the reasons leading to a successful SE attack?
- Does the susceptibility to SE attacks differ based on the national culture of targets?
- Does the susceptibility to SE attacks differ based on the organizational culture of targets?
- Does the susceptibility to SE attacks differ according to employee's personality traits?
- How can we utilize the findings in an organizational context?

To answer our research questions, we conducted a comprehensive literature review on SE-related literature as well as studies revolving around cultural influence. We aimed to define a correlation between the studied factors and the SE triggers and map these factors in regard to their influence on their correlated elements. We used a layered approach with our evaluation of the factors of the framework. Such an approach focuses on the effect of each layer on the next one. As a result, we managed to establish a framework that maps the susceptibility to SE attacks with cultural factors by proxy. Moreover, we proposed a practical framework aimed at measuring the susceptibility in each organization to develop better educational and training programs.

2.2 Suggested Framework to Measure the Influence of the Three-Layered Factors

Our research on existing literature indicates that there is hierarchical influence among three layers of factors. The features of a national culture can have its impact on shaping the cultural values of an organization within. Also, the set of values of a certain organization is reflected upon the behavior of its employees. Therefore, the susceptibility of employees to social engineering attacks may be higher or lower based on the environment of these employees, nationally and within the organization.

Because of that, we claim that it is very useful to evaluate the relationships of these factors with the social engineering psychological triggers to develop a more comprehensive understanding of such attacks and how to better handle them.

Regardless of the fact that a direct correlation of cultures and security awareness might appear to be difficult, we should not disregard their influence on human behavior within the context of security awareness (Übelacker, S., 2013). Therefore, we will utilize our conclusions, and apply them to a framework designed for the purpose of providing a mechanism to improve the susceptibility of employees in an organization.

2.2.1 The Impact of National Culture on The Organizational Culture

Even though it is possible to measure the correlation between the national culture factors and the SE triggers, it is more convenient for us to avoid cultural bias to first analyze their impact on the organizational culture, which shapes the behavior of the establishment employees or potential targets. National cultures provide a frame in which organizational cultures function (Übelacker, S., 2013). Values and norms defining national cultures must be considered when we evaluate organizational culture factors. To do that in our research, we are going to discuss the impact of each national cultural factor on the factors comprising the organizational culture by mapping each influential factor to its influenced organizational factor.

Based on existing research, it has been widely noted that there exists a relationship between national and organizational cultures (Schneider, B., & Smith, D. B., Eds., 2004). Westwood (1992) states in his work the consequences of the national cultural dimensions scores on the organizational level. His findings explained the relationship of each dimension on the organizational norms and behaviors. Additionally, there are significant influences of culture on the work values which have been proved by the paper of Claes and Ruiz-Quintanilla (1998) when we take into consideration the dimensions introduced by Hofstede (1991).

A. Power Distance

Upon analyzing the Power Distance dimension (PDI), we discovered that it substantially affects three organizational dimensions namely level of control, dimension of focus and the management philosophy dimension. PDI can influence the organizational culture with regard to the dimension of the level of control. High power distance encourages a strict

work discipline, while low scores would be catering for the creation of easy-going discipline. The subordinate and supervisor in large power distance countries have large emotional distance between them which disheartens the subordinate of getting guidance by the supervisor. On the ither hand, the working relationships in small power distance countries are more confirmed and there are communication, skill-development behaviors, and networking (Masouras, & Papademetriou, 2014).

PDI also can relate to the dimension of focus as high scores promote local-based focus, and low scores would lead to professional-based. In high power distance countries, organizational structures are very centralized with clear levels of managers and subordinates and tall hierarchies (Hofstede, 2001).

The management philosophy dimension is affected as well by PDI, where high scores influence a work-oriented philosophy, and low scores would promote the reverse. According to Hofstede (2001), countries with high PDI influence organizations where managers depend on formal rules and guidance to manage using an authoritative managerial style and decision making.

Table 4 Power Distance Impact on Organizational Culture

Organizational Culture Dimensions	High Power Distance	Low Power Distance
Level of Control	**Strict Work Discipline** • The subordinate and supervisor have big emotional distance between them. • The subordinates are discouraged of getting advice by the supervisor.	**Easy-Going Discipline** • The working relationships are more promoted. • There are skill-development behaviors, communication, and networking.
Focus	**Local-Based Focus** • Organizational structures are very centralized. • Tall hierarchies and clear levels of managers and subordinates.	**Professional-Based Focus** • Flat organizational hierarchies. • Decentralized structures.
Management Philosophy	**Work-Oriented Philosophy** • Managers rely on formal rules to manage. • Authoritative managerial style and decision making.	**Employee-Oriented Philosophy** • Managers rely on personal experience. • More consultative or collaborative forms of decision making.

B. Uncertainty Avoidance

It was noted that national cultures with high uncertainty avoidance (UAI) have a positive impact on the organizational effectiveness dimension. A low value of uncertainty avoidance is more likely to lead to mean-oriented organizational cultures. On the other hand, a high score of uncertainty avoidance would contribute towards more goal-oriented workplaces. Countries with weak uncertainty avoidance are open to new ideas, rewarding systems, and innovative behavior at the workplace. On the contrary, strong uncertainty avoidance nations are resistant to new ideas and innovation, and support workers' motivation using security (Masouras, & Papademetriou, 2014).

Additionally, UAI also contributes to the dimension of level of control. High UAI will influence a stricter work culture while low scores would influence the reverse. As stated by Hofstede (1986), nations with low uncertainty-avoidance are open minded and often try to minimize uncertainty. Therefore, they welcome new things and lifelong learning leading to an easy-going work environment.

Table 5 Uncertainty Avoidance Impact on Organizational Culture

Organizational Culture Dimensions	High Uncertainty Avoidance	Low Uncertainty Avoidance
Organizational Effectiveness	**Goal-Oriented** • Resistance to new ideas and innovation and support employee's motivation by security.	**Means-Oriented** > Openness to new ideas, innovative behavior, rewarding systems at the workplace.
Level of Control	**Strict Work Discipline** • Superiors are pessimistic about subordinate ambition. • Innovators feel constrained by rules. • Resistance to new things and lifelong learning.	**Easy-Going Discipline** • Acceptance of new things and lifelong learning which leads to an easy-going work environment.

C. Individualism vs. Collectivism

For the dimension of Individualism vs. Collectivism (IDV), its score would influence the dimension of customer orientation. A high IDV collective score is likely to create an internally driven environment, and high IDV individualistic scores influence an externally driven culture. Collective cultures would lead to a work culture in which workers act in the interest of the in-group, and their loyalty to the company is relatively low. Also, employee-employer relations are almost like a family bond. In individualistic nations, workers act in their interests, and their loyalty to the organizations is high.

Additionally, the employee-employer relationship is based on the market (Hofstede, 2001).

In addition to that, IDV would have the same influence on the dimension of level of control as collective cultures are easy-going in their work discipline and the opposite is leaning towards strict ethics. Howard et al., (1983) concluded that Japanese managers acquire social values in comparison to American managers who are individualists.

Also, IDV can be correlated to the dimension of focus. Collective cultures aspire for more local-focused organizational cultures, and individualistic ones push toward professional focus. Youn (2000) proved in his study that individualist nations like the United States have more powerful learning beliefs than collectivist nations like South Korea for the reason that individualism encourages the challenge to work.

IDV is also mapped to the dimension of approachability. Collectivism in a certain culture carries its effect to more open systems while individualism creates the inclination to closed systems. Hofstede (1991) states that in the workplace, the workers from individualistic countries are more independent, worry about them and plan future career. On the contrary, workers from collective nations are more open to training, sharing their skills, having good relationships and support common tasks.

Finally, IDV with high collective scores leads to establishing a work-oriented philosophy. High IDV individualistic scores indicate more focus on employee-oriented management philosophy. Hui and Yee (1999) proved in their study in Hong Kong that there are variations in job satisfaction and teambuilding amongst collectivist and individualist employees. Collectivists promote teambuilding while individualistic workers promote more job satisfaction. Kanungo and Wright (1983) showed that British managers assign more importance to independence and individual accomplishment than French managers. On the opposite, French managers give value to organization policies, security, expert management, and comfortable conditions in work.

Table 6 IvC Impact on Organizational Culture

Organizational Culture Dimensions	Individualism	Collectivism
Customer Orientation	**Externally Driven** • Employees act in their own interests. • Commitment to the organizations is high. • Employee-Employer relationship is based on the market.	**Internally Driven** • Employees act in the interest of in-group • Commitment to the company is relatively low. • Employee-Employer relationships are almost like a family link
Level of Control	**Strict Work Discipline**	**Easy-Going Discipline**

	• Managers are individualists in their relationships with employees. • Tasks and company prevail over personal relationships.	• Managers develop social values. • Better to reward based on equality (give everyone the same reward). • Support of teamwork.
Focus	**Professional-Based Focus** • Stronger learning beliefs. • Promotes the challenge to work.	**Local-Based Focus** • Employee-Employer relationships is almost like a family link. • Belief in collective decisions. • Personal relationships very critical in business.
Approachability	**Closed Systems** • The workers are more independent. • Workers worry only about them and plan future career.	**Open Systems** • Workers are open to training. • Open to share their skills. • Workers have good relationships and support common tasks.
Management Philosophy	**Employee-Oriented Philosophy** • Individualistic culture promotes job satisfaction.	**Work-Oriented Philosophy** • Give importance to company policies, security, expert management.

D. Masculinity vs. Femininity

In the masculinity vs. femininity (MAS) dimension, a feminine culture encourages an easy-going level of control while masculinity promotes a level of control that is strict relatively. Hofstede (2001) states that the employee's relationship with work in masculine cultures is based on living to work and seeking high pay. Moreover, workers look for security, high pay, and interesting work. While in feminine cultures, employees work in order to live, and they prefer to work for fewer hours. Also, workers look for better working conditions and relationships in work.

Moreover, MAS is an influencing factor on the dimension of approachability. High scores in femininity are very supportive of open systems in the corporate environment. However, based on analyzing the influence masculinity, it is likely that its effect on approachability may not be of relevance. According to Claes and Ruiz-Quintanilla (1998), masculinity deals with a challenging job, recognition, a chance for advancement to higher-level jobs, competition between colleagues and performance, wages, and career planning. Femininity cultures promote collaboration in work, security, and good working connections. Moreover, feminine cultures promote consultation, skill improvement, and

networking. These are practices that are promoted by small power distance nations as well.

As for the dimension of management philosophy, a feminine national culture can help shift the orientation of the management philosophy on the employees' side while masculinity can be inclined towards a job-oriented environment. Hofstede (2001) mentions that feminine cultures influence managers to be employees like others, and work problems are resolved by compromise and negotiations.

Table 7 MvF Impact on Organizational Culture

Organizational Culture Dimensions	Masculinity	Femininity
Approachability	**Closed Systems** • Challenging work, recognition, and opportunity for development to higher level jobs. • Competition among colleagues in performance and earnings. • Facilitates career planning.	**Open Systems** • Cooperation in work. • Security and good working relationships. • Consultation, skill development and networking.
Level of Control	**Strict Work Discipline** • Employee's relationship with work is based on living in order to work. • Seeking a high pay. • Workers look for security.	**Easy-Going Discipline** • Employees work in order to live. • They prefer to work for less hours. • Workers look for better working conditions and relationships in work.
Management Philosophy	**Work-Oriented Philosophy** • The company projects are prioritized over employees. • Conflicts are resolved through fighting until the best "man" wins.	**Employee-Oriented Philosophy** • Managers are influenced to be employees like others. • Work problems are resolved through compromise and negotiations.

E. Long-Term vs. Short-Term Orientation

To the best of our knowledge, the influence of the long-term vs short-term dimension on the organizational culture is not considered by other researchers. Intuitively, this dimension influences organizational cultures as nations develop commitments either on long-term or short-term. Have consistency, if use hyphen between long-term and short-

term have that everywhere. Long-term orientation focuses on the future by postponing short-term material or short-term emotional satisfaction. On the contrary, short-term orientation is when you are centered around the present or past and consider them more important than the future.

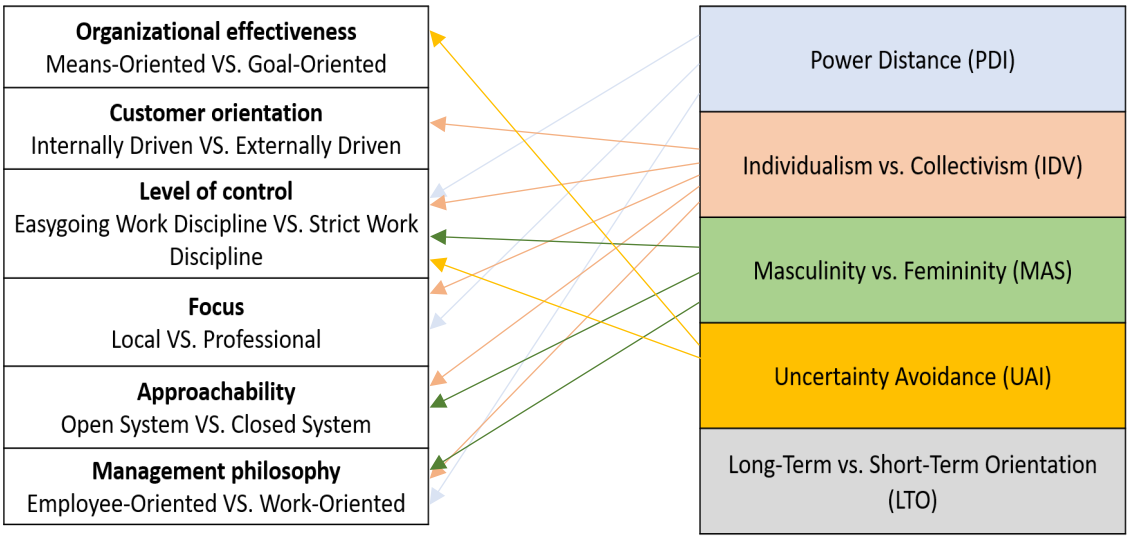

Figure 2 The Influence of National Culture on Organizational Culture

2.2.2 The Impact of Organizational Culture on Employee's Personality Traits

Factors such as organizational culture influence the shaping of the information security culture. Empirical studies have confirmed the impact of organizational culture on the culture of information security. On itself, information security culture is acknowledged as part of the corporate culture (Ruighaver, Maynard, & Chang, 2007), (Dojkovski, Lichtenstein, & Warren, 2006), (Schlienger & Teufel, 2005). Therefore, studying the impact of these factors can help to improve the overall security awareness of the organization. According to (Jedge and Cable, 1997), organizational cultures are linked to personality traits that respond to the attributes of organizational culture's factors. without doubt the organizational culture is linked to personality trait. Based on general understanding, we claim that organizational cultural dimensions influence personality traits. We intend to show the verification of our claim and calculation of that relationship score through empirical studies in the future.

A. Organizational effectiveness

This dimension is closely connected to the effectiveness of the organization. In a means-oriented culture, the key feature is the way in which work has to be carried out–the "how". In a goal-oriented culture, employees are primarily out to achieve specific internal goals or results–the "what".

This dimension opposes a concern with the means of doing the job to a concern with the goals set by organizations. In the means-oriented cultures, people regard themselves as dodging risks and giving only a little effort in their jobs, while living each day with the

same routine. In goals-oriented cultures, people recognize themselves as comfortable in unfamiliar conditions and put in a maximal work effort, while each day is considered to bring different challenges. It is challenging not to attach a "good" label to the goals-oriented side and a "bad" label to the other side for this dimension. However, organizations differ with their priorities based on the nature of their business.

B. Customer orientation

In a highly internally driven culture, employees perceive their task towards the outside world as a given, based on the idea that business ethics and honesty matter most. In a very externally driven culture, the only emphasis is on meeting the customer's requirements; results are most important.

This dimension deals with the popular assumption of customer orientation. Pragmatic units were market-driven, while normative units perceived their task in relation to the outside world. We can see that in the normative units, the major stress was on accurately following organizational plans, which were more important than results. In the pragmatic units, there was a major stress on satisfying the customer's requirements; outcomes were more valuable than exact procedures.

C. Level of control

This dimension refers to the amount of internal structuring, control, and discipline. A very easygoing culture reveals an internal fluid structure, a lack of predictability, and little control and discipline. A very strict work discipline reveals the reverse.

It relates to the volume of internal structuring in the organization. People in loose control units believed that no one thought of cost, the meeting time was only set approximately, and jokes about the business and the job were common. People in tight control units expressed their work environment as cost-conscious, meeting times were kept punctually, and jokes about the company and/or the job were limited.

D. Focus

In a local company, employees identify with the boss and/or the unit in which one works. In a professional organization, the identity of an employee is determined by his profession and/or the content of the job.

This dimension crosses units whose employees obtain their identity mainly from the organization to units in which people classify with their type of job. Members of parochial cultures considered that the organization's norms related to their behavior at home as well as on the job. They felt that in hiring employees, the company looked at their social and family background as much as their job competence. On the other hand, members of professional cultures viewed their private lives as their own affairs. They thought the organization hired on the basis of job competence only, and they did think far ahead.

E. Approachability

This dimension relates to the accessibility of an organization. In a very open culture, newcomers are made immediately welcome. In a very closed organization, it is the reverse.

Moreover, approachability opposes open systems to closed systems. In the open system units, members viewed both the company and its people as open to newcomers and outsiders. Nearly anyone would click into the organization, and new workers required only a few days to feel at home. In the closed system units, the organization and its workers were thought to be closed and reserved, even amongst insiders. Only very particular people fit into the organization, and new employees demanded more than a year to feel at home.

F. Management philosophy

In very employee-oriented organizations, members of staff feel that personal problems are considered. In very work-oriented organizations, there is heavy pressure to perform the task even if this is at the expense of employees.

This dimension crosses a concern for employees to a concern for completing the job. In employee-oriented cultures, workers felt that their individual difficulties were taken into account and that the organization took accountability for employees' welfare. Also, major decisions were initiated by groups or committees. In the job-oriented units, people encountered intense pressure to complete the task. They regarded the organization as involved only in the work workers did and not in their personal and family welfare. They perceive that important decisions were made by individuals.

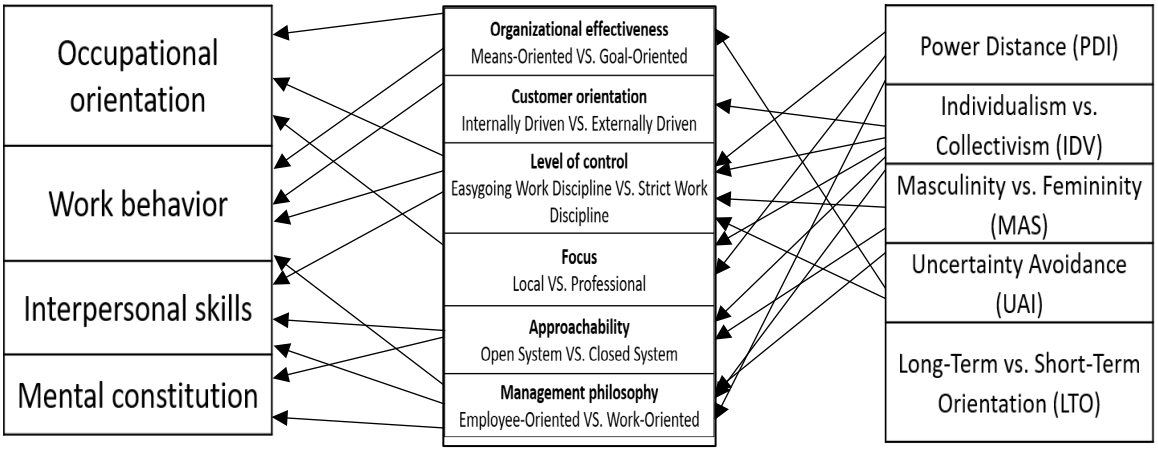

Figure 3 The Impact of Organizational Culture on Employee's Personality Traits

2.2.3 The Impact of Employee's Personality Traits on the Susceptibility to SE Attacks

A. Occupational Orientation

As occupational orientation defines the employees' ability to work at high standards and adhere to rules, they are vulnerable to methods that make use of social norms, policies, and rules. Continuance commitment, which is linked to occupational orientation, increases the vulnerability to SE. For example, even though people are concerned regarding their personal information, they would actively trade-off privacy for convenience as a result of a cost-benefit correlation to the benefits of perceived rewards (Uebelacker, & Quiel, 2014) & (Workman, 2008). Therefore, we suggest that it is correlated with the triggers: reciprocity, authority, and Integrity/consistency. It has also been declared that security training can reduce SE susceptibility, particularly for conscientious people (Parrish Jr et al., 2009).

B. Work Behavior

The level of flexibility in the employee's work behavior and his openness to new experiences would likely lead to an increased level of susceptibility to SE attacks. People with high openness values are less concerned about privacy issues connected to location-based services. These people's inclination to explore new experiences affects their risk evaluation (Junglas, & Spitzmuller, 2006). This can be conveyed to SE that free-minded people underrate the risk of becoming a victim and consequently do not exhibit sufficient coping strategies (Uebelacker, & Quiel, 2014). However, openness could lead employees to more technological proficiency which make them less vulnerable to SE attacks. As a result, we think that work behavior is only related to the trigger of strong affect for the reason of open people inclination to the belief of freedom of constraints.

C. Interpersonal Skills (Social Skills)

Employees with a high sense of trust tend to worry less about issues like privacy infringement. Extraversion is a defining factor in the interpersonal skills of employees. Extraverted people are considered a higher security risk (Darwish et al., 2012). Additionally, extraverted workers are more likely to infringe cyber-security policies, therefore, deciding to oppose policies to comply with suspicious and malicious requests (McBride et al., 2012). Weirich and Sasse (2001) show that employees who did not disclose their passwords, hence displaying a low level of SE susceptibility, are perceived as unsocial and distant by their co-workers, indicating low extraversion values. We can infer that the susceptibility of trusting people would be high since they would be willing to share private information with others based on established trust. Moreover, we predict their influence by the triggers: authority, reciprocity, and deceptive relationships.

D. Mental Constitution

One of the describing attributes to mental constitution is the level of agreeableness of employees, and their trust and confidence. "Agreeableness is possibly the personality trait that is most associated with phishing", and to a greater extent, social engineering (Parrish Jr et al., 2009). More agreeable people are at a higher chance of a security risk (Darwish

et al., 2012). Trust, a sub-trait of agreeableness, is assumed to mainly establish the relationship between agreeableness and SE susceptibility. An assumption that was shown in studies by (Weirich and Sasse, 2001) and by (Workman, 2008). Moreover, if the employee achieves low levels of the mental constitution, he would be more likely to be exploited as his confidence would fall. Nevertheless, more neurotic people are less likely to violate cyber-security systems (McBride et al., 2012). People low on self-images and with acknowledged paranoia are more likely not to reveal private information showing a low level of SE susceptibility (Weirich and Sasse, 2001). We expect hackers to engage the triggers of overloading, strong affect, diffusion of responsibility and moral duty, and integrity and consistency.

Table 8 The Impact of Employee's Personality Traits

Employee's Personality Traits	**Psychological Triggers of Social Engineering**	**Description**
Occupational Orientation	• Reciprocity • Authority • Integrity/Consistency	• Workers are vulnerable to methods that make use of social norms, policies, and rules. • People would actively trade-off privacy for convenience as a result of a cost-benefit correlation to the benefits of perceived rewards.
Work Behavior	• Strong Affect	• Free-minded people underrate the risk of becoming a victim. • do not exhibit sufficient coping strategies. • Open people are inclined to the belief of freedom of constraints.
Interpersonal Skills (Social Skills)	• Authority • Reciprocity • Deceptive Relationships	• Extraverted workers are more likely to oppose policies to comply with malicious requests. • Unsocial and distant workers display a low level of SE susceptibility.

		• The susceptibility of trusting people would be high.
Mental Constitution	• Overloading • Strong Affect • Diffusion of Responsibility and Moral Duty • Integrity and Consistency	• More agreeable people are at a higher chance of a security risk. • Employees with low levels of mental constitution, are more likely to be exploited as confidence would fall.

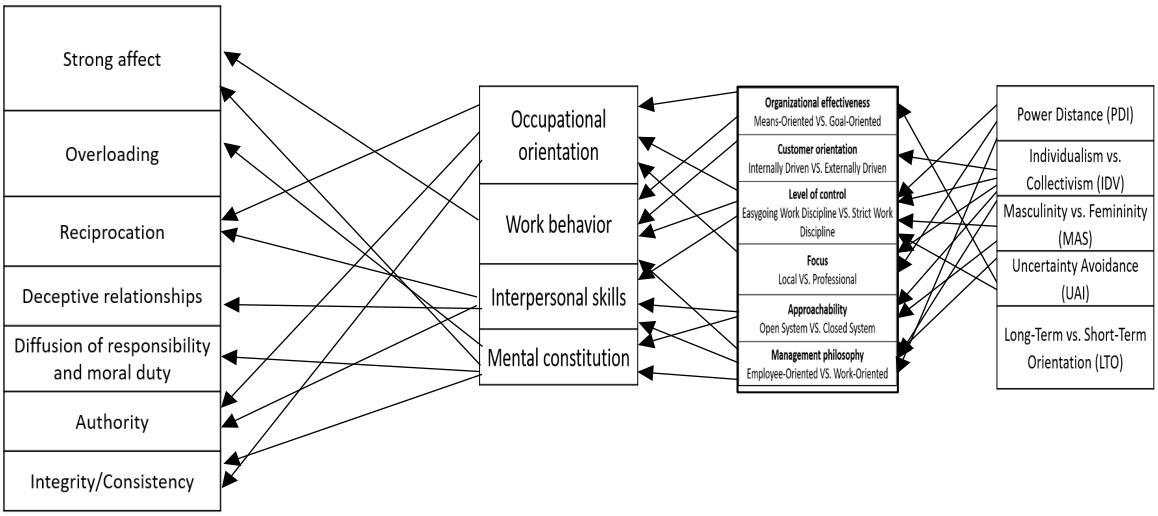

Figure 4 The Impact of Employee's Personality Traits on The Susceptibility to SE Attacks

2.3 Statistical Analysis of National Culture Influence

To validate the proposed framework, there is a need for an appropriate method of quantitative examinations of our framework's assumptions and hypothesis. The correlation of the studied factors and the susceptibility to SE attacks can be further confirmed using empirical data measured within the context of the factors of our suggested framework. Based on our research, there is a scarcity of available studies assessing the impact of cultural significance in SE attacks. Moreover, measured data extracted from empirical studies that can be used to set metrics for the factors influencing SE susceptibility are not available in abundance, with the exception of national cultural dimensions. Therefore, we will be conducting a statistical analysis only on the correlation of Hofstede's national cultural dimensions to SE susceptibility as it has been evaluated thoroughly in previous research. In addition, the analysis provided will provide a clear

vision of how practitioners can collect usable data on the rest of the framework, as well as having an implementable approach to measure the influence of culture within the context of SE.

Our analysis relied on the study made by (Sample et al., 2017), where they studied the victims of social engineering attacks as a group within the context of Hofstede's cultural framework to conclude whether particular cultural dimensions correlate with the victims of social engineering attacks. We relied on the data implemented in the study to test the groups as the paper extracted the data related to countries exploited by social engineering attacks between 2011 to 2014. The resources used to collect the data were: the Zone-H archive, Hofstede's cultural data values, and the World Internet Stats archive. The data were filtered to include SE attacks of countries measured by Hofstede's framework.

The Mann-Whitney-Wilcoxon (MWW) is a non-parametric statistical test used to compare two collections from the same population to evaluate the similarity of these two groups. In our case, we used this test to compare the victims and non-victims' countries. Our objective was to assess whether the victim and non-victim groups are culturally different from a statistical perspective. The probability value (p-value) that emanates from this analysis would be utilized for inferential purposes. We can conclude the statistical significance of the p-value if it is equal to 0.05 or less when executing this test.

H_0: From a cultural perspective, there are no statistical differences between victims and non-victims in a given year.

Testing the hypothesis H_0 was performed assuming the null hypothesis. The four-year window was investigated to decide whether longer-term patterns might exist. Therefore, yearly MWW tests and the Spearman correlation tests were done. The null hypothesis asserted that each group was statistically the same, suggesting that their distributions were identical. It can be described mathematically as H_0: H_1 $F(t) = G(t)$. One or more dimensions being statistically different with probability values of ≤ 0.05 is required for the rejection of the null hypothesis (H_0).

Equation 1 Statistical Difference Between Two Groups

$$G(t) = F(t - \Delta) \quad where, G \ \& \ F: Distribution\ Functions, t: Samples, \Delta: difference$$

Calculating the MWW relies on ordering the values from smallest to largest and calculating the sum of the values afterward. S_1 is the rank of the Y_1, and S_n is the rank of Y. The following equation shows how it is used.

Equation 2 Wilcoxon Signed Rank Test Formula

$$W = \sum_{j=1}^{n} S_j \quad where, W: Test\ Statistic, n: Sample\ Size, Sj: Rank\ j$$

A. Results

The data was collected and filtered based on the countries evaluated by Hofstede's model, and the type of attack where social engineering attacks were chosen. Out of the available dataset, we set the countries' lists based on records from the year 2014. The countries were divided into two groups: victims, non-victims, where victims refer to countries that are victims of social engineering attacks, and non-victims are the ones that did not receive social engineering attacks. The reason is to apply the MWW test and find the significance value of Hofstede's cultural dimensions.

The number of records collected before filtering by attack was 286103 records. After filtering by social engineering attacks, the records were 3932. The following table lists the number of countries and records collected from 2014.

Table 9 List of Countries & Records (Victims & Non-Victims)

Year	Number of Non-Victim Countries	Number of Victim Countries	No. of Records for Victim Countries (Non-SE Attacks)	No. of Records for Victim Countries (SE Attacks)
2014	25	62	282171	3932

Table 10 Victim Countries National Culture Values (retrieved from Hofstede Center.)

No.	Country	PDI	IvC	MvF	UAI	LvS	IvR
1	ALBANIA	90	20	80	70	61	15
2	ARGENTINA	49	46	56	86	20	62
3	AUSTRALIA	36	90	61	51	21	71
4	BANGLADESH	80	20	55	60	47	20
5	BELGIUM	65	75	54	94	82	57
6	BHUTAN	94	52	32	28	NA	NA
7	BRAZIL	69	38	49	76	44	59
8	BULGARIA	70	30	40	85	69	16
9	CANADA	39	80	52	48	36	68

10	CHILE	63	23	28	86	31	68
11	CHINA	80	20	66	30	87	24
12	COLOMBIA	67	13	64	80	13	83
13	CROATIA	73	33	40	80	58	33
14	CZECH.REPUBLIC	57	58	57	74	70	29
15	DENMARK	18	74	16	23	35	70
16	DOMINICAN.REPUBLIC	65	30	65	45	13	54
17	EGYPT	70	25	45	80	7	4
18	ESTONIA	40	60	30	60	82	16
19	FINLAND	33	63	26	59	38	57
20	FRANCE	68	71	43	86	63	48
21	GERMANY	35	67	66	65	83	40
22	GREECE	60	35	57	100	45	50
23	HUNGARY	46	80	88	82	58	31
24	ICELAND	30	60	10	50	28	67
25	INDIA	77	48	56	40	51	26
26	INDONESIA	78	14	46	48	62	38
27	IRAN	58	41	43	59	14	40
28	IRELAND	28	70	68	35	24	65
29	ISRAEL	13	54	47	81	38	NA
30	ITALY	50	76	70	75	61	30
31	JAPAN	54	45	95	92	88	42
32	KENYA	70	25	60	50	NA	NA
33	LATVIA	44	70	9	63	69	13
34	LITHUANIA	42	60	19	65	82	16
35	MALAYSIA	100	26	50	36	41	57
36	MEXICO	81	30	69	82	24	97
37	MOROCCO	70	46	53	68	14	25
38	NEPAL	65	30	40	40	NA	NA
39	NETHERLANDS	38	80	14	53	67	68

40	NEW.ZEALAND	22	79	58	49	33	75
41	NIGERIA	80	30	60	55	13	84
42	NORWAY	31	69	8	50	35	55
43	PHILIPPINES	94	32	64	44	27	42
44	POLAND	68	60	64	93	38	29
45	PORTUGAL	63	27	31	99	28	33
46	ROMANIA	90	30	42	90	52	20
47	RUSSIA	93	39	36	95	81	20
48	SAUDI.ARABIA	95	25	60	80	36	52
49	SERBIA	86	25	43	92	52	28
50	SINGAPORE	74	20	48	8	72	46
51	SLOVAKIA	100	52	100	51	77	28
52	SLOVENIA	71	27	19	88	49	48
53	SOUTH.AFRICA	49	65	63	49	34	63
54	SPAIN	57	51	42	86	48	44
55	SWEDEN	31	71	5	29	53	78
56	SWITZERLAND	34	68	70	58	74	78
57	TAIWAN	58	17	45	69	93	49
58	THAILAND	64	20	34	64	32	45
59	TURKEY	66	37	45	85	49	49
60	UK	35	89	66	35	51	69
61	VENEZUELA	81	12	73	76	16	100

Table 11 Non-Victim Countries National Cultural Values (retrieved from Hofstede Center.)

No.	**Country**	**PDI**	**IvC**	**MvF**	**UAI**	**LvS**	**IvR**
1	BURKINA.FASO	70	15	50	55	27	18
2	CAPE.VERDE	75	20	15	40	12	83
3	ECUADOR	78	8	63	67	NA	NA
4	EL. SALVADOR	66	19	40	94	20	89
5	ETHIOPIA	70	20	65	55	NA	NA

6	GHANA	80	15	40	65	4	72
7	GUATEMALA	95	6	37	99	NA	NA
8	HONDURAS	80	20	40	50	NA	NA
9	IRAQ	95	30	70	85	25	17
10	JORDAN	70	30	45	65	16	43
11	KUWAIT	90	25	40	80	NA	NA
12	LEBONAN	75	40	65	50	14	25
13	LIBYA	80	38	52	68	23	34
14	MALAWI	70	30	40	50	NA	NA
15	MOZAMBIQUE	85	15	38	44	11	80
16	NAMIBIA	65	30	40	45	35	NA
17	PAKISTAN	55	14	50	70	50	0
18	PANAMA	95	11	44	86	NA	NA
19	PERU	64	16	42	87	25	46
20	SENEGAL	70	25	45	55	24	NA
21	SYRIA	80	35	52	60	30	NA
22	TANZANIA	70	25	40	50	34	38
23	UAE	90	25	50	80	NA	NA
24	ZAMBIA	60	35	40	50	30	42

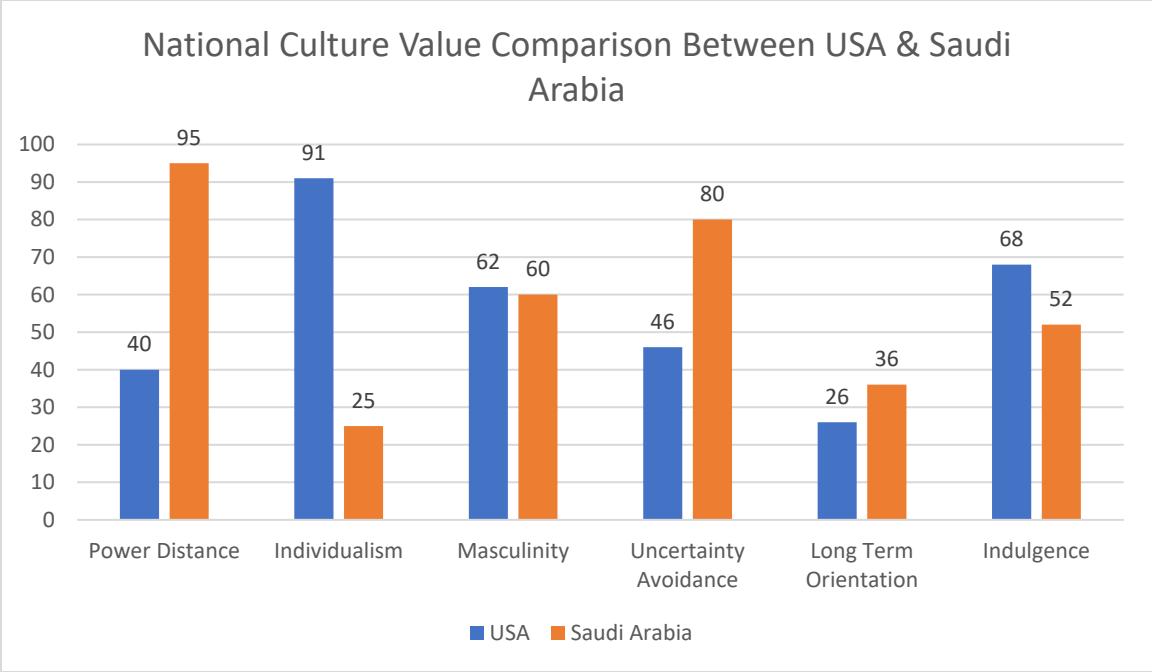

Figure 5 National Culture Value Comparison Between USA & Saudi Arabia (Retrieved from Hofstede Center.)

The next table shows the MWW test results between the social engineering victim and non-victim countries. Tests for statistically significant differences at the 5% (0.05) value or less are considered successful for statistically showing the existence of a difference. Test results that are between 5% and 10% are of interest but are not considered for the success criteria. The 5% to 10% values are determined to be of interest because human behavior is being measured and it has been observed that there could be an increase in the type II error when testing human behavior to 5% p-values. Type II error occurs when the researchers do not succeed in rejecting a null hypothesis which is actually false. The PDI, IvC, and LvS dimensions consistently showed significant differences between the victim and non-victim countries.

Table 12 MWW Comparison Between Victim & Non-Victim Countries

Year	PDI	IvC	MvF	UAI	LvS	IvR
2014	0.001975	0.00000749	0.2311	0.926	0.0001158	0.7741

The findings from the Wilcoxon test indicate significant correlation between the cultural dimensions and the victim countries which achieves the rejection of the null hypothesis. The results from the tests were, in some samples, unsurprising based on previous studies (Sample, 2015), (Karamanian et al., 2016), and (Sample & John, 2016). The IvC results state the effects of the group (Hofstede et al., 2010), (Bornstein, Kugler & Zieglemeyer, 2002). The cultural values seemed to display consistency in this dimension over long periods. As the victims' group developed over time, the comparison to the non-victims decreased, appearing in the overall that the victim group is progressing to the full

Hofstede population, yet the drawing toward individualist societies being victims and collectivist societies being non-victims persisted to be consistent. As a result, the individual yearly findings are very relevant.

The consistent findings in the PDI dimension are not only notable but also interesting given the fact that Hofstede et al. (2010) stated the relationship between authoritarian values that define high PDI societies and collectivism.

The LvS findings of long-term orientation suggest a possible motive to stay involved with the attacker or the impersonated character by the attacker. When coupled with low PDI and individualism characteristics, this may show a desire to discover more about the attacking side. The short-term orientation linked with non-victims implies that this group may carry the believe that the attackers will repeat attacking the organization in the future.

These findings indicate the relationship between culture and cyber behavior which shed the light on the importance of analyzing that relationship for an improved security awareness of organizations. Empirically, we need further studies to evaluate and measure the values of organizational culture and occupational personality traits in order to fully calculate the influence on external humanistic factors on the susceptibility of employees to SE attacks. The demand for more cultural examination of cyber behaviors is crucial. The consequences are vital in terms of training and awareness for SE potential victims.

Based on the same analytical tests, we can measure the significance of the other layers by collecting the values of these layers through empirical research. For example, let us assume that one dimension of the organizational factors was measured empirically for a number of organizations–for example, customer orientation. In this case, the organizations would be divided into two groups based on SE attacks–victims and non-victims. We will have numerical values of the customer orientation dimension, and two groups that we can name: sample 1 and sample 2. To measure the significance of this dimension on the susceptibility to SE attacks, the steps below are going to be used:

1. For each value in a sample of n items, obtain a difference score D_i between the two groups.
2. Then, ignore positive or negative signs and create a set of n absolute differences $|D_i|$.
3. Eliminate difference scores of zero, providing you a set of n non-zero absolute difference scores, where $n' \leq n$. Therefore, n' becomes the sample size.
4. Now, assign ranks R_i from 1 to n to each of the $|D_i|$ in a way that the smallest absolute difference score gets rank 1 and the largest gets rank n. If two or more $|D_i|$ are equal, they get assigned the average rank of the ranks they would have been assigned individually had ties did not occur.

5. Reassign the symbols "+" or "–" to each of the *n* ranks R_i, based on whether Di was previously positive or negative.
6. Subsequently, the Wilcoxon test statistic *W* is generated as the sum of the positive ranks.
7. We use the Wilcoxon value to calculate the probability denoted as the p-value for the reason of measuring the significance of the analyzed factor.

At the end, we would have a full statistical analysis of the factors influencing SE susceptibility, and their significance within the context of social engineering.

Chapter 3: Applying the Framework

3.1 Proposed Framework to Measure Susceptibility to SE Attacks

To practically use the findings of our suggested framework of the cultural impact, it is essential to provide a mechanism by which we can utilize the finding when measuring SE susceptibility of workers in the real life. For that reason, we are proposing a framework that security practitioners can use to engage the findings of the cultural impact when developing awareness and training programs for corporations. Our proposed framework is derived from Kevin Mitnick's attack cycle (Mitnick, & Simon, 2003) and its detailed structure is shown in Figure 5. This framework would computationally find weaknesses and susceptibility of employees in an organization and would create a personalized training and education program to raise employee's awareness against cybersecurity threats. Below we describe how each component of the framework works.

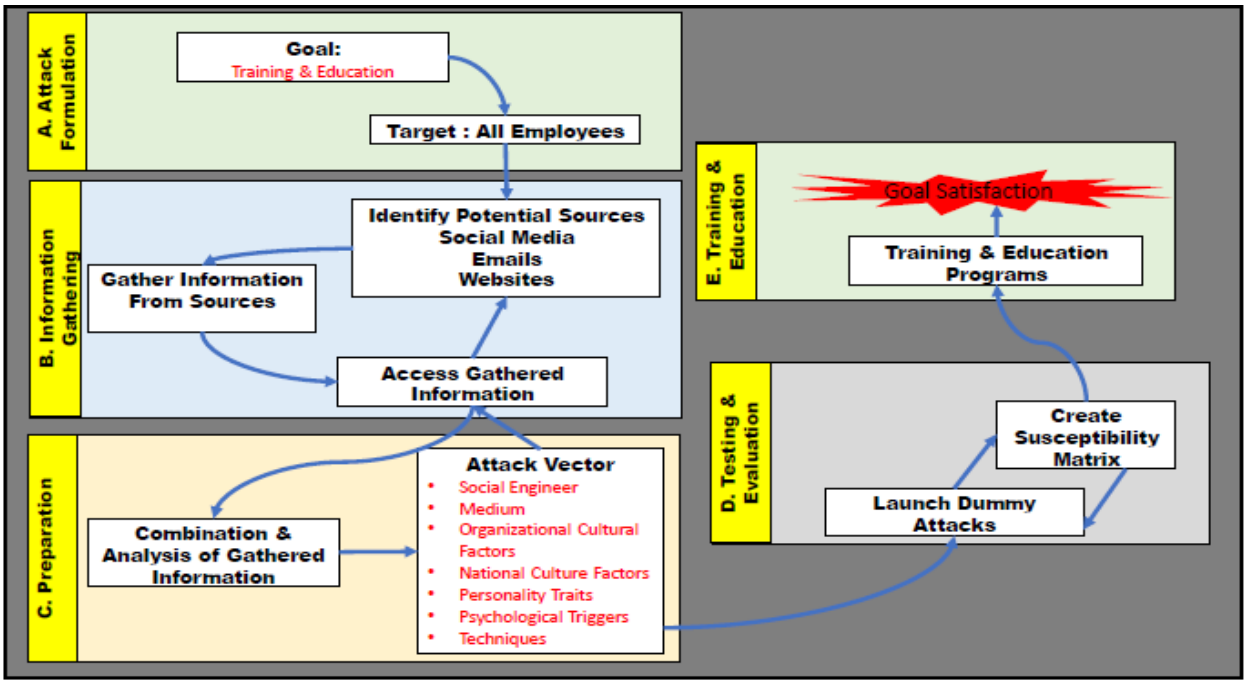

Figure 6 Components of the Proposed Framework

A. Goals and Target

As shown in Figure 6, in the first phase, the framework identifies the goals and the targets. All the employees of a national or international organization would be considered the target. And the main goal is to create a personalized training and education program based on the susceptibility of the employees to dummy SE threats.

B. Gathering Employee Information

In this step, information about the employees is gathered to support attack vectors. This step is very crucial for preparation, launching, and testing attacks. All possible sources from which the information can be obtained including company websites, social networking sites, phone calls, personal blogs/forums will be first identified. Next, tools such as Whois, nslookup, and keyhole would be used to gather all pieces of information (Wikipedia contributors., 2021), (Wikipedia contributors., 2021), and (Keyhole, 2021). All collected information would then be reviewed to gain intelligence into employee vulnerabilities. Note, the quality and quantity of information gathered about the target will determine the probability to obtain relevant results. If not much information is identified, then the scanning process will restart as shown in Figure 6. The fact that all it takes is "one employee user" to inadvertently open the gateway to social engineering attackers in the corporate sector necessitates this step. However, in order to protect the privacy of the employees, each employee information will be associated with a dummy name, and any data that identifies the identity of the employee will be removed or modified. If necessary, the collected information will be encrypted to preserve the privacy of the employees. Full measures will be taken to keep the employee data confidential and will not be misused in anyway. The key goal is to educate and train vulnerable users through customized training and education in order to protect the security of the individuals as well as the organization where he/she works and thus avoid the dangerous consequences of SE attacks.

C. Attack Preparation

All the collected bits and pieces of information about the employees are combined and used for framing all the common SE-attacks against which the users will be tested for susceptibility. Typically, a malicious actor commonly uses the following attack vectors to compromise the security of individual and organizations: phishing, vishing, credential harvester, impersonation, SMishing. In order to attack, dummy versions of these attack vectors will be generated using the Social-Engineering Toolkit (SET) (Kennedy, 2020). SET is an open-source penetration testing framework that allows the user to generate a believable attack quickly and test if the target lures into the target action. Let's say we are using this framework for a US-based company name "ABZ" which has two employees with alias names "Bob" and "Alice". The following example in Table 13, shows the national culture factors, organization culture factor along with the scores for each factor and employee information gathered in above step C. We use the scores for the national cultural factors using the Hofstede model, however since there is no study that measures the organization cultural scores the score is marked to be determined (TBD). Measuring organizational factor scores in outside the scope of this thesis and hence we will be

continuing this research in the future as we plan to conduct empirical study to determine these scores for certain companies within US and outside US. However, to show the crude design, here we show a toy example how the dummy attack would be launched based on randomly choose High and Low scores for customer orientation, level of control, focus and approachability factors as shown in Table 13.

Table 13 Example of Gathered Information

<table>
<tr><th>US National Culture Factors and Scores</th><th>Organizational Culture Factors and Scores for Company “ABZ”</th><th>Employee’s</th><th>Employee Gathered Information from Step C</th></tr>
<tr><td>Power Distance (Score 40)</td><td>Organizational effectiveness (Score: TBD)</td><td rowspan="2">Bob</td><td rowspan="2">Recently went for vacation to Hawaii; tweeted about confrontation with the manager; has two pet dogs; etc.</td></tr>
<tr><td>Individualism (Score 91)</td><td>Customer Orientation (Score: High)</td></tr>
<tr><td>Masculinity (Score 62)</td><td>Level of control (Score: Low)</td><td rowspan="4">Alice</td><td rowspan="4">Recent hire (~ 10 months of employment with “ABZ”, maintains a blog about faith and God; etc.</td></tr>
<tr><td>Uncertainty Avoidance (Score 46)</td><td>Focus (Score: Low)</td></tr>
<tr><td>Long Term Orientation (Score 26)</td><td>Approachability (Score: High)</td></tr>
<tr><td>Indulgence (Score 68)</td><td>Management Philosophy (Score: TBD)</td></tr>
</table>

Example attack 1: Individualism (High)--> Level of control (Low)-->Bob twitted about the confrontation with manager in social media --> launch a credential harvester attack (a fake email from the manager to Bob that he was fired with a sign-in link to see the details of the company policy to fire the employees).

Example attack 2: Individualism (High)--> Approachability (High)-->Alice maintains a blog about belief and God --> launch a phishing attack (a fake email from a church she regularly visits asking for donation by clicking a link).

As can be seen from above two dummy examples, attack vectors would include all the elements of SE attacks including organizational and national cultural factors. This is the attack plan which would enable the generation of a susceptibility matrix based on how the individuals respond to these dummy attacks.

D. Testing & Evaluation

In this step, a simulated/dummy attack created using SET toolkit is launched to lure the target into action. An effective pretext will withstand scrutiny and yet expose the vulnerabilities of the target. These dummy social engineering attacks will use manipulation tactics such as launching an email with long text followed by a hyperlink to click. This text would be crafted based on the information gathered in step B which evokes the target into remembering a bad or sad incident and subsequently feeling sad. Once the target is in the desired emotional state, there is a high probability that the target will click the malicious link that would create security holes in his system and turn the entire organization at risk. Another attack vector could exploit the faith of the employee. For example, sending targets emails purportedly from a legitimate church or mosque website urging them to visit the website, where they are requested to make small donations for the renovation of the building or something else of similar nature. The target would then give away the confidential information to the social engineer. Based on whether the target became victim or not the susceptibility matrix to attack vectors is generated.

E. Training & Education

Once the susceptibility is measured, customized security awareness training and education that would guide employees to take corrective measures to stop or reduce the impact of an SE attack will be recommended. This process would not stop once the goal of training and education is achieved rather this process would repeat itself periodically using new attack vector scenarios thereby creating strong human firewalls.

Chapter 4: Conclusion & Future Work

4.1 Conclusion

In this thesis, we discussed the impact of organizational cultural factors and personality traits on the susceptibility of employees to SE attacks. We demonstrate the relationship between those factors and the social engineering psychological triggers. Furthermore, we have shown how to use the assumed relationship in a given organization using a proposed framework that would detect the susceptibility and create an awareness program tailored for the employees' specific needs. We hope that the research initiated in this thesis will motivate other researchers to develop a more comprehensive understanding and measuring scores for organizational culture, personality traits factors and how each influence the other in better understanding social engineering attacks, and eventually design countermeasures and security awareness programs that are more effective in preventing SE attacks. During our research, we found out the scarcity of existing literature on the influence of such factors within the context of social engineering which

pose a challenge for corporates today to mitigate the damage of SE attacks. We conducted an analysis on the effect of national culture based on statistical tests. Such analysis could not be done for organizational culture influences since the scores for organizational culture is unfortunately not available in literature. Thus, in this thesis we cannot validate the working of our framework and hence we aim to do that in our future research by first conducting empirical studies measuring the scores for organizational culture factors.

4.2 Future Research Direction

The proposed framework in this thesis is theoretical and is still at the in the infancy stage of development. Extensive multi-year research is required to make this proposed framework fully functional and automatic before it can be adopted and benefit a security practitioner.

In this thesis, a deep analysis could not be conducted due to unavailability of scores for various factors for different layers. So, the first part of our future research will involve conducting empirical experiments to collect data from various companies within US and outside US. We anticipate that this will be a many years project and require collaboration with companies and other research collaborators. We will first start with small pool of companies within US and slowly expand it to companies outside US. After the scores are determined, we will conduct more empirical experiments to validate mapped relations between the factors and the psychological triggers. At first, in a simulated organizational setup, real human subjects will be invited to participate for crude analysis and automation of the framework. After which our goal is to conduct real experiments in a real organization by initiating research collaboration with the companies. The impact of organizational and national culture will be measured through questionnaires based on existing models of Hofstede Cultural Dimensions and Multi-Focus Model on Organizational Culture. The occupational traits of employees will be measured using the Business-focused Inventory of Personality (BIP). Based on these models, a metric will be designed to evaluate the performance of the subjects. Then, the result will be analyzed to compute the weight and scores of employees.

These computed scores would be used during the designing of our simulated SE attack in order to give focus to the techniques and methods that increase the susceptibility of the employees. The components of the framework will be set according to the computed scores. As a result, we could analyze the outcome of the attack and evaluate the findings based on our calculated weight metrics. The computed values should give us an accurate evaluation of workers' susceptibility to SE attacks within the organization. Hence, mitigation strategies can be adjusted according to a specific group of workers. Knowing which factors modify the susceptibility to SE attacks will allows us to detect or even predict which kinds of attacks will be more likely to succeed in a specific personnel group which will aid in effective countermeasure steps such as team building, high-level

personalized awareness training, or rapid cultural transformation towards a security-aware organizational culture.

References

Algarni, A., Xu, Y., Chan, T., & Tian, Y. C. (2013, December). Social engineering in social networking sites: Affect-based model. In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)* (pp. 508-515). IEEE.

Allen, M. (2006). Social engineering: A means to violate a computer system. SANS Institute, InfoSec Reading Room.

Anon (2015) *Geert Hofstede Website* [online]. Available from: http://www.geerthofstede.nl/dimensions-of-national-cultures (Accessed 27 April 2021).

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences*, *1*(03), 23.

Bornstein, G., Kugler, T., & Ziegelmeyer, A. (2002). Individual and group behavior in the centipede game: Are groups (again) more rational players?. *Journal of Economic Literature C*, *72*, C92.

Burtner, W. K. (1991). Hidden pressures. *Notre Dame Magazine, Winter*, *92*, 29-32.

Claes, R., & Ruiz-Quintanilla, S. A. (1998). Influences of early career experiences, occupational group, and national culture on proactive career behavior. *Journal of Vocational behavior*, *52*(3), 357-378.

Darwish, A., El Zarka, A., & Aloul, F. (2012, December). Towards understanding phishing victims' profile. In *2012 International Conference on Computer Systems and Industrial Informatics* (pp. 1-5). IEEE.

Deal, T. E., & Kennedy, A. A. (1983). Corporate cultures: The rites and rituals of corporate life: Addison-Wesley, 1982. ISBN: 0-201-10277-3. $14.95. *Business Horizons*, *26*(2), 82-85.

Dojkovski, S., Lichtenstein, S., & Warren, M. (2006, January). Challenges in fostering an information security culture in Australian small and medium sized enterprises. In *The 5th European Conference on Information Warfare and Security proceedings. Reading, England, Academic Conferences* (pp. 31-40).

Fan, W., Lwakatare, K., & Rong, R. (2017). Social engineering: IE based model of human weakness for attack and defense investigations. *International Journal of Computer Network & Information Security*, *9*(1).

Flores, W. R., & Ekstedt, M. (2013). Countermeasures for Social Engineering-based Malware Installation Attacks. In *CONF-IRM* (p. 23).

GBC-DELL Survey. (2015). *The Human Factor at the Core of Federal Cybersecurity.* Government Business Council.

Gragg, D. (2003). A multi-level defense against social engineering. *SANS Reading Room*, *13*, 1-21.

Greavu-Serban, V., & Serban, O. (2014). Social engineering a general approach. *Informatica Economica*, *18*(2), 5.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.

Hadnagy, C. J., Aharoni, M., & O'Gorman, J. (2010). Social engineering capture the flag results defcon 18. *Retrieved October*, *30*, 2010.

Hofstede Center. *National Cultural Dimensions*. 2013. http://geert-hofstede.com/national-culture.html

Hofstede, G. (1980). Culture and organizations. *International studies of management & organization*, *10*(4), 15-41.

Hofstede, G. (1986). Cultural differences in teaching and learning. *International Journal of intercultural relations*, *10*(3), 301-320.

Hofstede, G. (1991). *Cultures and Organizations. Software of the Mind*. London: McGraw-Hill.

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Sage publications.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2005). *Cultures and organizations: Software of the mind* (Vol. 2). New York: Mcgraw-hill.

Hossiep, R., & Paschen, M. (2012). *Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung-6 Faktoren: Modul zur Selbstbeschreibung*. Hogrefe.

Howard, A., Shudo, K., & Umeshima, M. (1983). Motivation and values among Japanese and American managers. *Personnel Psychology*, *36*(4), 883-898.

Hui, C. H., & Yee, C. (1999). Workgroup Atmosphere on Chinese Employees' Job. *Applied Psychology: An International Review*, *48*(2), 175-185.

Judge, T. A., & Cable, D. M. (1997). Applicant personality, organizational culture, and organization attraction. *Personnel Psychology*, 50, 359–394.

Junglas, I., & Spitzmuller, C. (2006, June). Personality traits and privacy perceptions: an empirical study in the context of location-based services. In *2006 International Conference on Mobile Business* (pp. 36-36). IEEE.

Kanungo, R. N., & Wright, R. W. (1983). A cross-cultural comparative study of managerial job attitudes. *Journal of International Business Studies*, *14*(2), 115-129.

Karamanian, A., Sample, C., & Kolenko, M. (2016). Hofstede's cultural markers in successful victim cyber exploitations. *Journal of Information Warfare*, *15*(3), 7-23.

Kennedy, D. (2020). *trustedsec/social-engineer-toolkit*. GitHub. https://github.com/trustedsec/social-engineer-toolkit.

Keyhole, T. (2021, April 09). Hashtag analytics for Twitter, Instagram and Facebook. Retrieved April 28, 2021, from https://keyhole.co/

Leroch, M. A. (2014). Culture at work: how culture affects workplace behaviors. *International Journal of Manpower*.

Mann, M. I. (2012). *Hacking the human: social engineering techniques and security countermeasures*. Gower Publishing, Ltd..

Masouras, A., & Papademetriou, C. (2014). National Culture Underpins Individual Behaviour and Work-Related-Values: The importance of nationality.

Mataracioglu, T., & Ozkan, S. (2011). User awareness measurement through social engineering. *arXiv preprint arXiv:1108.2149*.

McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *RTI International-Institute for Homeland Security Solutions*, *5*(1), 1.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mittu, R., & Lawless, W. F. (2015, March). Human Factors in Cybersecurity and the Role for AI. In 2015 AAAI Spring Symposium Series.

Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A personality based model for determining susceptibility to phishing attacks. *Little Rock: University of Arkansas*, 285-296.

Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A personality based model for determining susceptibility to phishing attacks. *Little Rock: University of Arkansas*, 285-296.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Security Journal*, *15*(5), 13.

Pfleeger, C. P., & Pfleeger, S. (2006). Why we won't review books by hackers. *IEEE Annals of the History of Computing*, *4*(04), 9-9.

Ross, S. (2006). *A guide to Social Engineering: Vol. Volume 1* [E-book]. http://www.astalavista.com/index.php?section=directory&cmd=detail&id=3487

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & security*, *26*(1), 56-62.

Rusch, J. J. (1999, June). The "social engineering" of internet fraud. In *Internet Society Annual Conference, http://www. isoc. org/isoc/conferences/inet/99/proceedings/3g/3g_2. htm*.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: a survey. *Future Internet*, *11*(4), 89.

Sample, C. (2015). *Cyber+ culture early warning study*. CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States.

Sample, C., & John, M. (2016, June). Cultural Comparison Between and Attackers and Victims. In *ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security* (p. 269). Academic Conferences and publishing limited.

Sample, C., Hutchinson, S., Karamanian, A., & Maple, C. (2017, June). Cultural observations on social engineering victims. In *16th European Conference on cyber-security and Warfare,(Dublin: University College Dublin)* (pp. 391-401).

Scheeres, J. W. (2008). *Establishing the human firewall: reducing an individual's vulnerability to social engineering attacks*. AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT.

Schlienger, T., & Teufel, S. (2005, May). Tool supported management of information security culture. In *IFIP International Information Security Conference* (pp. 65-77). Springer, Boston, MA.

Schneider, B., & Smith, D. B. (Eds.). (2004). *Personality and organizations*. Psychology Press.

Scholz, C. (1987). Corporate culture and strategy—The problem of strategic fit. *Long Range Planning*, *20*(4), 78-87.

Smith, A., Papadaki, M., & Furnell, S. M. (2013). Improving awareness of social engineering attacks. In *Information Assurance and Security Education and Training* (pp. 249-256). Springer, Berlin, Heidelberg.

Social engineering (political science). (2021, March 21). In *Wikipedia*. https://en.wikipedia.org/wiki/Social_engineering_(political_science)

Stergiou, D. (2013). *Social Engineering and Influence: A Study that Examines Kevin Mitnick's Attacks through Robert Cialdini's Influence Principles*.

Übelacker, S. (2013). *Security-aware organisational cultures as a starting point in mitigating socio-technical risks*. Gesellschaft für Informatik eV.

Uebelacker, S., & Quiel, S. (2014, July). The social engineering personality framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24-30). IEEE.

Uebelacker, S., & Quiel, S. (2014, July). The social engineering personality framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24-30). IEEE.

Vigilante. "Social Engineering." *Security Resources*. No date. URL: http://www.vigilante.com/inetsecurity/socialengineering.htm.

Watkins, M. (2013). What is organizational culture? And why should we care. *Harvard Business Review*, *15*.

Weirich, D., & Sasse, M. A. (2001, September). Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 137-143).

Westwood, R. I. (1992). Culture, cultural differences, and organisational behaviour. *Organisational behaviour: Southeast Asian perspectives*, 27-62.

Wikipedia contributors. (2021, April 6). WHOIS. In *Wikipedia, The Free Encyclopedia*. Retrieved 07:08, April 28, 2021, from https://en.wikipedia.org/w/index.php?title=WHOIS&oldid=1016287362

Wikipedia contributors. (2021, February 2). Nslookup. In *Wikipedia, The Free Encyclopedia*. Retrieved 07:08, April 28, 2021, from https://en.wikipedia.org/w/index.php?title=Nslookup&oldid=1004484564

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.

Youn, I. (2000). The culture specificity of epistemological beliefs about learning. *Asian journal of social psychology*, *3*(1), 87-105.