SOCIAL ENGINEERING: HOW U.S. BUSINESSES STRENGTHEN THE WEAKEST LINK AGAINST CYBERSECURITY THREATS

by

Lily J. Pharris

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University, School of Business

August 2019

Abstract

The purpose of this transcendental phenomenological qualitative study was to investigate how IS professionals working in U.S. businesses make sense of their lives and experiences as they address and prevent vulnerabilities to social engineering attacks. This larger problem was explored through an in-depth study of social engineering and its effect on IS professionals working in U.S. businesses operating within healthcare, financial services, and educational industries across the central and northwest regions of Louisiana. Through its use of a phenomenological research design, the study bridged a gap in the social engineering literature, which was primarily comprised of studies that utilized a quantitative methodology. The use of a qualitative approach allowed participants to give voice to their beliefs, thoughts, and motivations about the work they do. The findings, consisting of ten themes and two subthemes, present the essence of experience of six IS professionals addressing and preventing social engineering vulnerabilities in their workplace. The findings revealed that the lived experience of protecting an organization from social engineering attacks involves the unification of people across the enterprise to develop a strong security-minded culture. Additionally, participants shared two primary beliefs, (1) that social engineering attacks would never be eradicated and (2) that IS professionals depend on everyone in the organization to protect the organization from social engineering attacks. The study offers recommendations to IS professionals, business leadership, HR professionals, educators, consultants, vendors, and researchers.

Key words: social engineering, vulnerability, weak human link, IS professional beliefs, security culture.

SOCIAL ENGINEERING: HOW U.S. BUSINESSES STRENGTHEN THE WEAKEST LINK AGAINST CYBERSECURITY THREATS

by

Lily J. Pharris

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University, School of Business

August 2019

_____

Dr. Gayle Jesse

_____

Dr. Allen Harper

_____

Dr. Edward Moore

_____

Dr. Dave Brat

Dedication

To my children, my entire world. Always remember, the best way to eat an elephant is one bite at a time.

Acknowledgements

I would like to thank my magnificent dissertation chair, Dr. Gayle Jesse, for her unwavering support, guidance, and encourage through each stage of the research and writing process. Thank you for embracing me as your student and mentoring me as we inched along together towards our end goal. I cannot imagine having tackled this monumental and overwhelming journey without you. I'm also exceedingly grateful to Dr. Gene Sullivan for identifying the perfect chair for me, as this decision made all the difference in my successful progression throughout this tedious and painstaking process.

I also wish to acknowledge both the DBA director, Dr. Edward Moore, and my committee member, Dr. Allen Harper, for their quality feedback during those critical check-ins along the way. Thank you for seeing the potential in my topic and helping me make it the best it could be. Additional thanks goes to Dr. Brat, Dr. Calland, and the LUDBA faculty and staff who helped me achieve each milestone along the way to a degree in my cognate area of Computer Information Systems.

I would also like to extend a special thanks to Northwestern State's Dr. Margaret Kilcoyne, Dean of the College of Business and Technology and Dr. Curtis Penrod, Coordinator of the CIS program. Thank you for understanding when I needed to prioritize my pursuit of this degree program above other activities. Your support was instrumental in helping me accomplish this goal in three years. Appreciation also goes out to the CIS and School of Business faculty at NSULA who empathized, encouraged, inspired, and assisted me any time I asked. I could not ask for a better work-family.

The goal of this project could not have been accomplished without the willingness of six wonderful IS professionals who opened up about their experiences with the phenomenon. You

know who you are, but you may never realize how grateful to you I am. A hundred times over, thanks.

One does not embark upon this journey alone, and I am so grateful for the friendships established with Holly, Karen, Chad, and other students I met along the way. Your kind words, shared struggles, and ongoing prayers kept me connected and motivated me to finish.

There have been so many sacrifices made by family and friends supporting me through this process. Thanks to everyone who understood when I had to forego our time together to write and meeting deadlines. And, to my parents, Nelda and Glen Jeane, you have always been there to provide the love and support I needed in life, but somehow you stepped everything up another notch while I pursued this dream. Without you stepping in to watch Keegan and Klara, this project would have taken much longer or ended before it began. I can never thank you enough. I am looking forward to the time we get to spend making up for the rushed or missed visits from the last three years. Gabriel, Clint, Rachael, Nathaniel, Cheryl, Sonny, and Lindsey—thank you for believing in me and offering your encouragement and listening ear when I needed it. I appreciate you.

And last, but not least, Paul Pharris, my love. We did it. You received the brunt of me, often at my worst, and you still took everything in stride. Thank you for embracing the changes it brought to our lives and coming out the other side stronger because of it. Thank you for bringing magic into my world the moment we met. I love you, and I look forward to making more magic together as we look ahead together at whatever comes our way next.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

What good is a lock, if someone leaves the door open? What good is a password, if the password is shared with the wrong person? When a company invests millions of dollars in the most secure, state-of-the-art technology to protect itself, but fails to equip the people interacting with the technology, the business and its assets remain vulnerable to social engineering attacks (Manske, 2000). As of the current study, research has not paid attention to what the experience is like for cybersecurity professionals as they address social engineering-related risks. Instead, a considerable amount of research has focused on the defensive tactics that should be employed if a business hopes to reduce the risk of various cyber threats, including social engineering (Albladi & Weir, 2018; Happ, Melzer, & Steffgen, 2016; Indrajit, 2017; Flores & Ekstedt, 2016; Nohlberg, 2018; Hinson, 2008). Indeed, very little has been understood about whether IS professionals believe it possible to eliminate the human-related vulnerabilities that are so adeptly targeted by social engineers. This study was designed to address this lack of understanding.

The purpose of this phenomenological qualitative study was to investigate how IS professionals working in U.S. businesses make sense of their lives and experiences as they address and prevent vulnerabilities to social engineering attacks. This study contributes to the body of knowledge by discovering commonly shared experiences, attitudes, motivations, and beliefs of IS professionals who defend businesses against social engineering threats. Understanding the essence of what it means to protect an organization from social engineering threats provides insights into other contributors to social engineering vulnerabilities in U.S. businesses beyond the well-documented weak-human link (Huber, Kowalski, Nohlberg, & Tjoa, 2009; Indrajit, 2017; Mann, 2017). Furthermore, the results of this study may be used by

business leadership and IS personnel to support greater investment in strengthening the human link against social engineering attacks.

Section 1 includes the background of the problem, problem statement, purpose statement, nature of the study, research questions, conceptual framework, definitions of important terms, assumptions, limitations, delimitations, the significance of the study, and a review of the professional and academic literature.

Background of the Problem

While most organizations consider people to be their greatest asset, those working in the field of cybersecurity acknowledge that people also represent one of their greatest security threats (Dahbur, Bashabsheh, & Bashabsheh, 2017; Parsons, McCormac, Butavicius, & Ferguson, 2010). As the sophistication, application, and goals of social engineering attacks have advanced over the last decade, cybersecurity professionals have been tasked with fully protecting the organization, especially against those threats targeted at its people (Hatfield, 2018). In 2017, Jackson found that IS professionals recognize additional education and training are needed for anyone at risk for exploitation; even so, IBM found in its 2016 Cybersecurity Index Report that 60% of successful cybersecurity incidents originated from an insider human source (IBM, 2016). This divergence between the acknowledgement of the demand for education and training and the ongoing exploitation of human capital suggests that more research is necessary to help businesses understand more about how companies are actively strengthening the human link against social engineering attacks. Indeed, if U.S. businesses cannot address the weakest link in the chain of defense against social engineering, costly attacks will continue to leave information systems and the data they house open to costly exploitation by offenders with malicious intent (Ponemon Institute, 2017). The current body of literature provides important clues about how

and why social engineers target an organization or individuals within an organization in the first place (Albladi & Weir, 2018; Happ et al., 2016; Indrajit, 2017).

Status of social engineering research. Businesses, IS professionals, and researchers have access to a plethora of knowledge across the body of literature in terms of useful techniques to help them understand, measure, and guard informational assets against social engineering attacks (Flores & Ekstedt, 2016; Nohlberg, 2018; Hinson, 2008). As a result of these extensive efforts, everyone stands to benefit from the availability of research aimed at helping businesses develop greater awareness of the various tactics used by social engineers (Tetri & Vuorinen, 2013; Mann, 2017; Hasan, Prajapati, & Vohara, 2010). Researchers have also spent time investigating the role and importance of security awareness on individuals across an organization (Bauer, Bernroider, & Chudzikowski, 2017; Torten, Reaiche, & Boyle, 2018). Certainly, the study by Dahbur et al. (2017) indicated a concern for the lack of security awareness displayed by the people of an organization. Yet this deficit of exhibited security awareness behavior does not necessarily mean security awareness training efforts have not taken place. In fact, researchers recognize that security awareness training may be occurring, but not all security awareness training methods are equally effective (Junger, Montoya, & Overink, 2017; Caldwell, 2016). Understanding the role of security awareness, the tactics social engineers use to target individuals and companies, and the defensive strategies businesses have at their disposal are all very useful as organizations develop effective responses to looming social engineering threats. Still, as successful social engineering attacks persisted in the workplace, it became even more important to identify gaps in body of the literature that have not yet been fully reported on.

Gaps in the literature. Most social engineering research studies utilize a quantitative design, which is unable to offer the same depth of understanding that qualitative designs allow

(Stake, 2010). The use of a qualitative research design is critical if researchers hope to advance the literature towards a deeper understanding about what may be occurring within the business that allow risks and vulnerabilities so often targeted in social engineering attacks to persist. This study attempted to bridge the gap in the literature by utilizing a qualitative approach to take a closer look at the lived experience of IS professionals who work on the front lines of cyber defense across U.S. businesses.

Shared experiences, challenges, and responses. In addition to utilizing a qualitative lens to bridge the gap in the literature, this study is an essential contribution to the body of literature because of its focus on sharing the essence of common experiences of IS professionals as they work in different industries to protect the organization against persistent and ever-evolving social engineering attacks. According to He, Devine, and Zhuang (2018), information sharing in cybersecurity helps to reduce the damage caused by cyberattacks, to reduce the overall number of cybersecurity incidents, to increase the effectiveness of a response due to the greater shared understanding, and to reduce the overall cost related to cyber defense by limiting or eliminating the duplication of efforts. The findings of this study can be used inform businesses and cybersecurity professionals about shared experiences and challenges, and at the same time reveal how different businesses are responding to social engineering challenges in their own way. Sharing the essence of what it is like to safeguard an organization against social engineering threats can offer valuable insights into how some companies are able to successfully thwart the attempts of incoming social engineering attacks, while other companies remain susceptible.

Shared attitudes and motivations. Lastly, gaining a greater depth of understanding about what it is like to be a cybersecurity professional exposed more about the attitudes and motivations held by practitioners. The current body of literature offers limited information as to

whether practitioners feel they have the necessary support, resources, and training to adequately do the job they have been hired to do. This study attempted to close this gap in the literature by highlighting any attitudes or perceptions that may present previously unexplored challenges that need to be addressed before U.S. businesses can minimize their susceptibility to socially engineered attacks.

Problem Statement

The general problem addressed in this study is that U.S. businesses are still vulnerable to costly social engineering attacks even though many information systems have advanced enough to diminish the loss of data and other proprietary information from cybersecurity threats (Flores & Ekstedt, 2016; Applegate, 2009; Shoniregun, Dube, & Mtenzi, 2014; Junger et al., 2017). The specific problem addressed by this study is the deficit of understanding about how IS professionals make sense of their lives and experiences as they address and prevent vulnerabilities to social engineering attacks while working at businesses operating in the healthcare, financial services, and higher education sectors in the central and northwest regions of Louisiana. Researchers and IS professionals readily agree that people are the weakest link in the chain of defense against social engineering attacks (Huber et al., 2009; Indrajit, 2017; Mann, 2017). Even businesses with the strictest security measures in place remain susceptible to incursion, because employees, with their natural tendency to trust other people, are fair game and prime targets for manipulation by social engineers (Mouton, Leenen, & Venter, 2016; Granger, 2001). To make matters worse, social engineers no longer need to be physically present to exploit the human vulnerability of an organization (Fan, Lwakatare, & Rong, 2017).

Purpose Statement

The purpose of this transcendental phenomenological qualitative study was to investigate how IS professionals working in U.S. businesses make sense of their lives and experiences as they address and prevent vulnerabilities to social engineering attacks. This larger problem was explored through an in-depth study of social engineering and its effect on IS professionals working in U.S. businesses operating within healthcare, financial services, and educational industries across the central and northwest regions of Louisiana.

Nature of the Study

The study was conducted using transcendental, phenomenological qualitative research design because the aim of the research is to better understand how IS professionals working in U.S. businesses make sense of their lives and experiences related to social engineering attacks. Interviews were conducted with IS professionals working in healthcare, financial services, and higher education industries within businesses operating in the central and northwest regions of Louisiana. The interview questions concentrated on discovering commonly lived experiences and the essence of the lived experiences of the phenomenon of IS professionals defending against social engineering vulnerabilities within U.S. businesses. Response data were analyzed by the researcher to formulate themes from participant responses to the questions asked during the interview. Themes were developed for all research questions.

Discussion of method. This section provides a brief description of four qualitative approaches to inquiry, narrative, case study, grounded theory, and phenomenology. Following the description, a rationale is presented as to why each approach was selected or rejected as appropriate for this study. Ethnographic research is excluded from consideration due to the

cultural anthropologic nature of the approach, which lies are outside the expertise of the researcher.

Narrative. Narrative research centers on the understanding of experiences (Clandinin & Caine, 2008), making narrative designs especially beneficial for researchers who wish to delve into the particularities of an individual or group experience. Stories and descriptions are often studied and reported as a series of events that took place in a unique contextual situation (Pinnegar & Daynes, 2007). Narrative studies typically report stories of experiences from the perspective of a single person or multiple individuals, and within a structured narrative, and investigators focus closely on the lives of individuals to extract important meaning from the story that is being shared (Creswell & Poth, 2018; Creswell, 2014). Stories often intimately explore the conversations, dialogue, situations and nuanced sensations elicited from interactions between study participants and the researcher who interprets and elicits meaning from these interactions. Narrative studies place great emphasis on understanding an experience from the perspective of individuals, but not every individual experience is relevant and relatable to public audiences (Clandinin, 2016). This study attempted to understand the common meaning of a shared experience of IS professionals defending an organization against social engineering attacks. Because the focus of this study hinges on the shared perspective of a group of people rather than the individual experiences, the narrative approach to inquiry was ruled out.

Case study. Often, case studies are used as a way for researchers to describe how the chosen case depicts a specific issue (Creswell, 2014). An investigator selects a case, or multiple cases, and illustrates how some identified problem occurs in an existing, real-world scenario (Creswell & Poth, 2018). Case studies are presented and considered within a specific time, place, and topic, which creates the context of a bounded system that constrains the research

effort. The primary goal of the case study approach tends to be a prepared case description and themes, and it is most appropriate to use when the researcher holds minimal, and preferably zero, power to control or influence behavioral events and outcomes (Yin, 2014). Additionally, a case study is more appropriate when the focus of the study deals with a current phenomenon, rather than a historical case. While case studies are applicable for studies dealing with a unique phenomenon, group, or individual, the aim of the current research effort focuses less on the context, cause, or reason of the phenomenon than a case study. For this reason, case study research was deemed an inappropriate mode of inquiry for the current study.

Grounded theory. Grounded theory research is characterized by its focus on the generation or discovery of a theory (Strauss & Corbin, 1997; Stake, 2010). In grounded theory design, the researcher develops theories by grounding them in data elicited from individuals or groups that have experienced some process or action (Creswell & Poth, 2018). As such, in grounded theory, the investigator takes the perspectives of many study participants to create some abstract or generalized explanation of a chosen process, action or interaction. Thus, it appropriate for a researcher to use the research design of grounded theory when they wish to advance or identify a theory. Because the current study primarily aimed to understand a shared experience rather than to develop new and emergent theories about the processes and actions taken by IS professionals dealing with social engineering attacks, grounded theory design was not appropriate for the research effort.

Phenomenology. Phenomenological research is used to uncover what a shared experience means for those persons who have experienced a phenomenon (Moustakas, 1994). Phenomenological research does not attempt to explain the cause or reason behind the phenomenon; rather, it simply endeavors to describe a complete account about the essence of the

experience of those who lived the phenomenon. The phenomenological point of view is often used to emphasize the meaning that people assign to the people and things that surround them (Krathwohl, 2009). As follows, if a person's reality is indeed shaped by social constructs, "to reach a full understanding of the purpose of a person's behavior it is necessary to see the world through their eyes" (Krathwohl, 2009, p. 242). In this study, the phenomenon is the experience of IS professionals working to prevent social engineering vulnerabilities in U.S. businesses. The phenomenological research methodology was been deemed an appropriate research design, because this approach to inquiry is used to ascribe a common meaning to a lived experience of a phenomenon for several persons (van Manen, 2016b).

Hermeneutic phenomenology. Within the phenomenological approach resides hermeneutic phenomenology (van Manen, 2016a) and transcendental phenomenology (Moustakas, 1994). The hermeneutic method considers phenomenology through systematic reflection on the lived experience through the perspective of the person living through the experience (van Manen, 2016a). The eventual outcome of using this methodology is a complete description or interpretation of the experience. Additionally, the underlying philosophical assumptions of phenomenological research tend to be based on the study of lived experiences of individuals and the belief that the persons are consciously aware of these lived experiences (van Manen, 2016a).

Transcendental phenomenology. In contrast, the transcendental method presents the experiences of the study participants, rather than the interpretations of the researcher (Moustakas, 1994). In transcendental phenomenology, researchers try to pull out, or bracket, personal experiences and notions to gain insight from the fresh perspective of the participants (Creswell & Poth, 2018). The investigator analyzes and codes the data, eventually developing themes that

convey the spirit of the experience shared by participants. The transcendental methodology better captured the purpose of this study as it allowed the researcher to convey the essence of the experience of the participants rather than the interpretations of the researcher.

Discussion of design. This study employed a qualitative research design. Qualitative research designs differ from quantitative designs in that a qualitative design attempts to discover an explanation and understanding (Stake, 2010). Unlike quantitative studies which lean heavily on the use of numbers to predict and control study outcomes and to convey meaning from a distinct phenomenon (Krathwohl, 2009), the spirit of qualitative studies differs due to "the integrity of its thinking. There is no one way of qualitative thinking, but a grand collection of ways: it is interpretative, experience based, situational, and personalistic" (Stake, 2010, p. 31). Whereas the role of a researcher in quantitative studies is impersonal, the role of the qualitative researcher is personal.

Greater insights. Qualitative research methods allow an investigator to observe ordinary, day-to-day happenings to better understand the meaning underlying this selected phenomenon. In qualitative research, the investigator plays a part in the study, as an instrument that observes, interviews, and examines the articles and documentation collected during the study. As it was the desire of this research study to emphasize greater insights into the essence of the experience of faculty members as they prepare students for the workforce, the qualitative research design provided the appropriate means by which this could be accomplished.

Summary of the nature of the study. In sum, this study employed a transcendental, phenomenological, qualitative design. The purpose of this study was to develop a greater understanding about the common experiences of IS professionals working to prevent social engineering vulnerabilities in U.S. businesses, which a qualitative design allows more than a

quantitative design. Of the narrative, case study, grounded theory, and phenomenological research methods, phenomenological methods provided the best way for a researcher to understand the shared experiences of a group of people working in the same role across different industries. Just as important, phenomenological methods accomplished this task without attempting to discover the cause or reason for the problem being addressed by the study, which was outside the bounds of the current research effort. Within the phenomenological design, the transcendental design methods enable a researcher to capture the essence of a phenomenon from the perspective of study participants, rather than relying on the interpretation of the researcher, as seen in the use of hermeneutic research methods. Thus, the transcendental method was selected as most appropriate for this project.

Research Questions

The following research questions were investigated:

RQ1: What lived experiences do IS professionals have with preventing social engineering vulnerabilities in U.S. businesses?

RQ2: What is the essence of the shared experience of IS professionals in preventing social engineering vulnerabilities in U.S. businesses?

RQ3: What common meaning do IS professionals ascribe to the experiences of preventing social engineering vulnerabilities in U.S. businesses?

RQ4: What role do circumstances play in the methods chosen by IS professionals working in U.S. businesses to decrease security vulnerabilities related to human manipulation?

Conceptual Framework

The social engineering defensive framework (SEDF), as described by Gardner and Thomas (2014), was used as the basis for the conceptual framework of this qualitative,

phenomenological research study. SEDF is grounded in the belief that technology and user training alone cannot prevent social engineering attacks. Furthermore, SEDF outlines a process that can be utilized by organizations to determine how well they are currently positioned against social engineering attacks, so businesses can prevent such attacks from being successful. The process consists of four phases, including (a) determine exposure, (b) evaluate defenses, (c) educate the workforce, and (d) streamline existing technology and policy. The study was also informed by concepts related to anticipatory cybersecurity, behavioral change, and organizational behavior.

Anticipatory cybersecurity. Unlike the ineffective, response-driven approach to cyberattack management, the concept of anticipatory cybersecurity centers on businesses strategically using tactical defense measures to anticipate and manage the attack strategies of highly trained, persistent adversaries (Rege, 2016). Businesses that use anticipatory defense measures can offset social engineering attacks by applying the same dynamic and adaptive tactics that attackers typically use against them (Rege et al., 2017). Rege (2016) argued that if IS professionals expect to design and implement anticipatory cybersecurity measures, they must understand who and what they are up against. By understanding their adversaries, IS professionals then can build the requisite, critical infrastructures to effectively defend against social engineering incidents. Still, to accomplish this feat, IS professionals will require significant resources and support from their company leadership, which not every business may sufficiently provide due to diverse constraints.

Beliefs, attitudes, and behavioral intention. Research on the social and work behaviors of people in various fields of study revealed that human behaviors are influenced by an individual's beliefs, attitudes, and behavioral intentions (Fishbein & Ajzen, 1975; Ajzen, 1991;

Mishra, Akman, & Mishra, 2014; Godin, Bélanger-Gravel, Eccles, & Grimshaw, 2008). Furthermore, research has shown that a person's behavior can be predicted by the attitudes and behavioral intentions currently held by that individual (Ajzen, 1991). Fishbein and Ajzen's (1975) behavioral intention model, the Theory of Reasoned Action (TRA), has been used by researchers to examine and explain the link between attitudes and human behavior. TRA offered support for the current study by establishing the importance of understanding beliefs, attitudes, and behavioral intentions of IS professionals, as these factors can help investigators understand and predict the behaviors IS professionals engage in to prevent social engineering attacks.

Occupational stress. This study was also informed by the idea that occupational stress influences worker performance. Presently, businesses struggle with finding and hiring an adequate number of qualified cybersecurity professionals to address the countless threats aimed at penetrating the technological and physical defenses of the business (Reagin & Gentry, 2018). Additionally, businesses also depend heavily on their IS team to help build sustainable competitive advantage in their industry. The initiatives undertaken to create this advantage tend to result in increased job demands and responsibilities for CIS professionals (Messersmith, 2007). Occupational stress has been associated with workers who engage in work situations where job demands are high, job control is low, and support is low (Johnson & Hall, 1988; Karasek, 1979; Karasek & Theorell, 1990; Salanova, Peiró, & Schaufeli, 2002; Moen et al., 2016). The resultant emotional exhaustion from dealing with occupational stress has been linked to reduced worker productivity (Donald et al., 2005).

Moore (2000) identified work overload as the greatest contributor to exhaustion in technology workers. Interestingly, the IS professionals in the Moore (2000) study recognized the primary reason for work overload and exhaustion emanated from the deficient staff and

inadequate resources available for performing assigned job duties. More recently, Agbonluae, Omi-Ujuanbi, and Akpede (2017) argued that once again occupational stress is a concern for workers and hindrance to worker productivity in industry. The present study allowed the researcher to examine the role that occupational stress plays in the lives of IS professionals attempting to thwart social engineering attacks, thus providing further insight into the situational context of the experience. Additionally, the study also enabled the researcher to scrutinize the reasons vulnerabilities related to social engineering continue to persist, which offered insights into how organizations might reprioritize strategic resources to address any deficits.

Discussion of relationships between concepts. Successfully implementing social engineering prevention strategies within organizations involves more than installing technology and training users (Gardner & Thomas, 2014). Following SEDF and proactively anticipating cybersecurity and social engineering attacks requires trained IS professionals who have access to everything they need to design and implement the critical infrastructures that will effectively defend against the countless attacks aimed at the organization they are attempting to defend (Rege, 2016). Presently, there are not enough workers to fill all the cybersecurity jobs openings across business and industry (Reagin & Gentry, 2018), and those who are trained and working in industry may be experiencing higher occupational stress from the higher job demands and stressors (Messersmith, 2007). Occupational stress has been shown to affect attitudes and intentions and to increase worker exhaustion (Moore, 2000), and occupational stress has negative implications for job productivity (Agbonluae et al., 2017). Beliefs, attitudes, and behavioral intentions influence individual behavior (Fishbein & Ajzen, 1975). Hence, to truly understand why the human vulnerability to social engineering attacks remains, a closer look at the context surrounding the situational circumstances and experiences of IS professionals working to defend

their company against adversarial attacks and the beliefs, attitudes, and behavioral intentions of these professionals was needed. The current study attempted to address this need. The conceptual framework delineates how the study concepts interact with one another within the IS department, as it is situated within the overall organization, is illustrated in Figure 1.

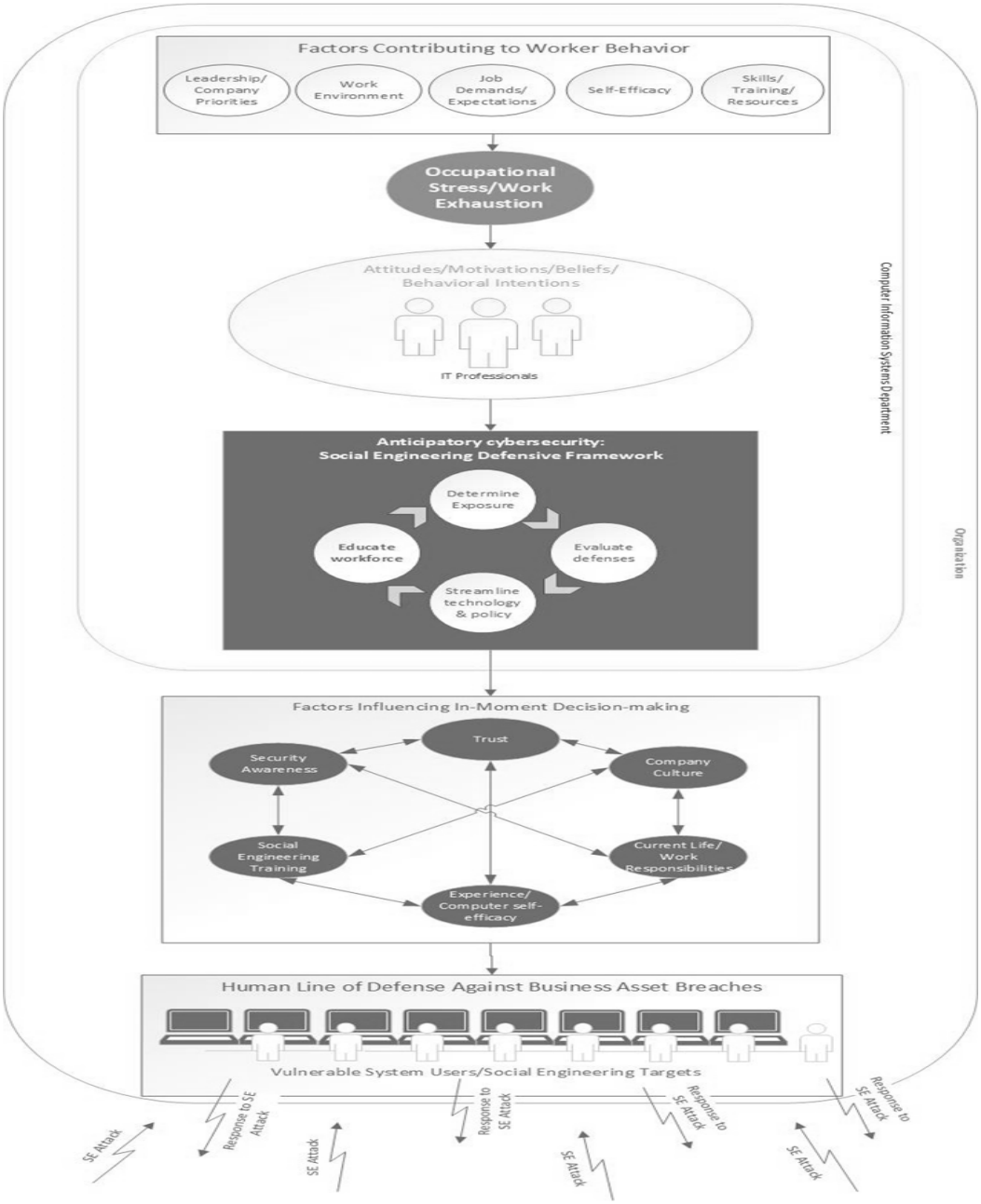

Figure 1. Conceptual framework.

Summary of the conceptual framework. The researcher designed the conceptual framework in Figure 1 to delineate how the concepts interact with one another within the IS department, as it is situated within the overall organization. Company and leadership priorities, environmental factors, work expectations, self-efficacy, and the availability and access to resources each have an effect of the organizational stress and work exhaustion experienced by individual IS professionals. The organizational stress and work exhaustion experienced by each IS professional shapes the individual attitudes, motivations, beliefs, and behavioral intentions towards the work produced by that individual and the IS department.

In the context of the study, the attitudes, motivations, beliefs, and behavioral intentions of IS professionals help determine the quality and quantity of anticipatory cybersecurity utilized across a company to strengthen the most vulnerable areas from social engineering attacks. The framework suggests that following the SEDF process leads to fulfillment of the concept of anticipatory cybersecurity. As anticipatory cybersecurity measures infiltrate the organization, it influences the factors used by people during spur of the moment decisions—the types of decisions often preyed upon during social engineering attacks. The response given to socially engineered attacks by the human front line of defense during that split-second decision-making moment of the request is dependent on the confluence of all the factors interplaying during that moment. This study highlights the importance of understanding what goes on in the lives of IS professionals, because what happens with these workers eventually determines how well the company can stand resolutely against imminent social engineering threats.

Definition of Terms

Terms deemed critical to understanding the current study are defined. Potentially unfamiliar or ambiguous terms are also described.

Anticipatory cybersecurity: The use of proactive cyber defense tactics that enable an organization to prepare for sophisticated cyber strikes using deliberate attack strategies (Rege, 2016).

Business email compromise (BEC): A sophisticated scam perpetuated by a criminal using social engineering techniques via email to pose as a legitimate person (i.e., company official, executive, etc.) to seek unauthorized payments or access to confidential employee information (FBI Internet Crime Complaint Center [FBI IC3], 2018).

Computer-based fraud: An act of deceit typically assisted by technology or the internet that is easily committed with minimal cost and considerable anonymity (Dolan, 2004).

Cyberattack: A well-planned, coordinated activity to modify, interrupt, mislead, damage, or destroy computer networks, systems, or the software or information residing on or sent through these networks or systems (National Research Council, 2009).

Cybersecurity: The composition, arrangement, and assembly of resources, practices, and structures used to protect the computer-related cyber systems from cyberattacks (Craigen, Daikum-Thibault, & Purse, 2014).

Hacking: Any unauthorized access or intrusion into a computer system or network; any crime committed via or against a computer (Pipkin, 2003).

Incursion: See cyberattack.

Malware: Any software, script or code maliciously added to a computer device, system or network that changes its condition or purpose without consent of the owner (Verizon, 2013).

Occupational stress: Stress related to the workplace that occurs when a difference exists between the demand of the work and a person's ability to fulfill these demands (Agbonluae et al., 2017).

Phishing: A commonly used social engineering tactic that utilizes email or the internet to solicit and steal restricted information (Luo, Brody, Seazzu, & Burd, 2011).

Pretexting: A commonly used social engineering tactic that utilizes a made-up scenario to coax a possible victim to volunteer information or carry out an action (Luo et al., 2011).

Security (Information Security): An educated determination, awareness and sense of assurance that information risks and security controls are stable (Anderson, 2003).

Security awareness: The cognizance and recognition of IT security concerns that help a person to respond appropriately to security risks or threats (National Institute of Standards and Technology [NIST], 1998).

Security control: Any safeguard or countermeasure specified for a business or information system aimed at protecting the privacy, reliability, integrity, and accessibility of its information (FIPS PUB 199 [FIPS], 2004).

Social engineer: An individual who employs tactics that appeal to or manipulate human emotions to persuade victims to grant them unauthorized access to computer systems or networks for illicit purposes (Workman, 2008b).

Social engineering: The "clever manipulation of the natural human tendency to trust with the intent to obtain information that will allow the unauthorized access to a valued system and the information that resides on that system" (Nagy, Hale, & Strouble, 2010, p. 260).

Social engineering defense framework (SEDF): A framework conceived to support the efforts of businesses to prevent social engineering attacks (Gardner & Thomas, 2014).

Spear-phishing: A cyberattack where an attacker performs research to better understand an identified target, designs a realistic email and phishing website, and attacks the target with the

intent of gaining unauthorized access to computer systems or networks (Caputo, Pfleeger, Freeman, & Johnson, 2014).

Work exhaustion: Job burnout (Moore, 2000).

Work overload: High work demands that exceed the capacity of a worker (Weigl et al., 2016).

Assumptions, Limitations, Delimitations

Assumptions, limitations, and delimitations are important, because each helps to identify potential weak points within a research effort. Assumptions reveal any underlying beliefs held by the researcher, limitations clarify constraints of the chosen methodology and study design, and delimitations designate the bounds of the study by articulating what the study will include and exclude (Simon & Goes, 2013). All assumptions, limitations, and delimitations have the potential to affect study outcomes; therefore, it is important to consider the role each plays within the study. Assumptions, limitations, and delimitations for the present project are described in the subsequent paragraphs.

Assumptions. Clarification of assumptions supports an effective appraisal of the analysis, synthesis, and conclusions of a study (Wolgemuth, Hicks, & Agosto, 2017). Accordingly, the following conditions were assumed true for the purposes of this study. While participants were expected to be representatives of their business, they did not necessarily represent all their industry or of all organizations/industries in the United States. It was assumed that participants possessed sufficient knowledge and experience with social engineering to provide legitimate and meaningful insights about their personal beliefs, attitudes, and perceptions related to protecting the business from social engineering threats. It was also assumed that participants gave their best effort to provide honest and accurate responses to all questions during

the interview process. To encourage honest and accurate responses, identifiable information about study participants and employers were withheld from publication. Study participants were not forced to answer any questions that made them uncomfortable. Additionally, study participants were given the opportunity to review the transcript of the interview and provide feedback and clarification to ensure their responses were accurately captured.

Limitations. Study limitations include any systematic bias the investigator could not, or chose not, to control in the study (Price & Murnan, 2004). Limitations have the potential to influence study results. First, as a phenomenological research, study participants were asked to articulate thoughts and perceptions about social engineering. The study was limited by how well participants express their personally held thoughts and perceptions. Second, the study was limited by the nature of phenomenological research, where the aim is only to seek to understand the phenomenon of IS professionals working to prevent social engineering attacks and vulnerabilities in U.S. businesses, meaning the results will not lead to the creation of theories about why the phenomenon of social engineering persists. Third, the background of the investigator may have influenced the types of interview and follow-up questions posed to study participants and the interpretation of participant responses. Last, while steps were taken to maintain the anonymity of participants, so they feel they are able to provide honest and accurate responses to all questions during the interview process, the interviewer had no control over the actual responses of participants. Additionally, like most qualitative studies, the researcher interpreted participant responses, leaving the study results susceptible to researcher bias during the data investigation and interpretation stages.

Generalizability. According to Creswell (2014), good qualitative research is characterized by particularity more than generalizability. Accordingly, the current study limited

its focus to the main types of social engineering interactions (i.e., phishing, pretexting) that occur within the business environment, making the study results less generalizable to situations outside the business context. Moreover, because study participants were limited to a small geographic area, study results may be less generalizable to areas outside the region being explored. Also, the small sample size may not accurately reflect practices and views of other organizations, or organizations operating in different industries, in the United States or other countries. Furthermore, only human vulnerabilities related to employees at a business were considered. In many industries, social engineers also target other individuals (i.e., students, stakeholders, etc.) for access to business systems. Findings of this study may not be generalizable to non-employees.

Delimitations. Delimitations include any systematic bias the researcher purposefully included in the study design to contain the scope of the research effort (Price & Murnan, 2004). The group of participants were limited to IS professionals currently working to protect their organization from cybersecurity attacks, with preference given to workers with experience addressing social engineering issues. Because U.S. businesses have unique organizational structures, the study participants were limited by whether the IS professional is considered a 'security' professional, but the participant must have been actively working in a computer-related or technology-based profession to be eligible for participation. Demographic factors, like age, ethnicity, or race that have the potential to influences beliefs and attitudes towards social engineering were excluded from the study.

Sector and region. The study was limited to IS professionals working for healthcare, financial services, and higher education businesses in central and northwest regions of Louisiana. The findings from these industries may not be applicable to all IS professionals working for

businesses operating outside healthcare, financial services and higher education or in other regions. Nor should results be broadly applied to all IS professionals working for any businesses within the central and northwestern regions of Louisiana. While it is expected the three selected industries and the geographic region under investigation will influence participant responses, the goal of the study is to understand the phenomenon from the perspective of industry professionals. Accordingly, the discovery process primarily focused on the commonly shared experiences within the identified industries and region. Still, the researcher inspected reasons for response differences between the sectors within the investigation if they appeared during the discovery process. The scope of the study did not attempt to explore differences between sectors or regions outside the current investigation.

Significance of the Study

"Social engineering is the lever that fraudsters are using to penetrate organizations and commit big dollar crimes—and no amount of anti-virus protection is going to defend against these sophisticated targeted attacks" (Field, 2016, p. 2). According to Information Systems Audit and Control Association's 2016 State of Cybersecurity Survey, social engineering is the first method cybercriminals, responsible for most attacks on business, utilize to initiate an attack on a company. Increasingly, the straightforward social engineering tactics are sophisticated enough to enable attackers to hide in plain sight (Internet Security Threat Report [ISTR], 2017). Furthermore, since all it takes is one click of a malicious email phishing link to gain access to confidential business assets or employee credentials, any common employee can be a potential target (Verizon, 2018; Positive Technologies, 2018).

Fraud and business. In PwC's 2018 Fraud Survey, cybercrime, the success of which often hinges on effective social engineering, was more than twice as likely to be identified as the

most disruptive type of fraud to a business (Lavion, 2018). And attacks are not expected to slow down (Information Systems Audit and Control Association [ISACA], 2016). The digitally enabled world has allowed the scale and impact of fraudulent activities, like social engineering, to grow considerably, making a lack of awareness and understanding within an organization exceedingly dangerous (Lavion, 2018). Incidents continue to escalate, leading to damaging consequences for the brands, reputations, and economic situation of companies who fall prey to social engineering schemes.

Employee credentials. In the 2016 Email Security Social Engineering Report, 65% of surveyed organizations that fell victim to social engineering discovered the attacks started with compromised employee credentials (Ponemon Institute, 2017b). Retrieving employee credentials is the first task on the way to the launch of a business email compromise (BEC) strike and committing fraud or theft at the company. The impact of such strikes is felt across the entire business (Verizon, 2018b). BEC reports to the FBI resulted in upwards of $3.1 billion in fraud losses between October 2013 and May 2016 (Field, 2016). According to Verizon's 2018 Data Breach Investigations Report, the cost of cybercrime will reach $2 trillion by 2019, and no industry is immune from its impact. Moreover, being a small or medium sized business does not exempt an organization from being targeted (Proof Point, 2018; Ponemon Institute, 2017b). In fact, in 2017, well-known cybercriminal groups have turned their gaze to target smaller organizations, which often have fewer security measures for them to overcome (Proof Point, 2018).

SMBs and security control measures. The findings of this study may be especially relevant for smaller- and medium-sized businesses (SMBs), which do not have access to the same human capital or budgetary resources as larger enterprises. Ponemon Institute's 2017 State

of Cybersecurity in Small and Medium Businesses Survey reported that SMBs are being attacked more than ever, and SMB personnel, budgets, and technologies are insufficient to create the necessary stronghold to withstand an attack. On top of facing more attacks than ever before, nearly half (49%) of security leaders responding to the 2016 Email Security Social Engineering Report felt the current controls employed by their company were either average or below average. In the same survey, 69% of respondents said the volume of social engineering attacks increased over the previous year. In a time where the sophistication and quantity of social engineering attacks are ramping up, average and below average control measures will not keep company doors open.

Executive support. Cybersecurity and information security are not just problems for the IS and operations team to address. Indeed, 94% of security leaders responding to the 2016 Email Security Social Engineering report say concerns surrounding social engineering are warranted, if not the most significant threat faced by business (Field, 2016). The same security leaders agree that user awareness efforts tend to be ineffective, leaving the organization vulnerable to attacks. IDG's 2016 Global State of Information Security Survey revealed that nearly half (43%) of security leader respondents see CEOs and board members making cybersecurity a top business risk.

Everyone's problem. Reports suggest that executive support is the least of their concerns (PwC, 2018; ISACA, 2016; Verizon, 2018b; Field, 2016), implying that executive teams realize cybersecurity involves every part of business, not just the IT-related areas of business. Because anyone at an organization may be targeted using social engineering tactics, and the impact of a breach can be detrimental to the entire organization, social engineering is a problem that must be dealt with across the entire enterprise. The following sections show how the current study

addresses the identified gaps in the literature, offers implications for biblical practice, and relates to the field of CIS.

Reduction of gaps. This study attempted to reduce the gap in the literature by concentrating on the dearth of understanding about what it is truly like for an IS professional working to protect a business from social engineering attacks. The existing body of literature lacked information about whether IS workers feel they have the necessary support, resources, and training to effectively do the job they have been hired to do. The current study is important because it provided greater insight into the readiness, willingness, and ability of an IS department to utilize SEDF, or other continuous improvement techniques, to design, implement, and maintain anticipatory cybersecurity defense measures to sufficiently offset social engineering attacks. Looking at the same problem from a different perspective can open opportunities for new ways to understand the same situation (Sandberg, 2000). The design of this study facilitated a different way of looking at and learning from a phenomenon than how it was already understood throughout the current body of literature. The investigation offered a rich description of the experience so that meaning could be derived from any commonly shared beliefs, attitudes, and behavioral intentions of IS security professionals, given their existing company and leadership priorities, environmental factors, work expectations, self-efficacy, and the availability and access to resources.

Implications for biblical integration. Social engineering, at its core, is a lie being targeted at the vulnerable areas of a business (Airehrour, Nisha, & Madanian, 2018). Lying is a sin (Deuteronomy 20:16. New International Version), and sin not only separates people from God (Isaiah 59:2), but sin also has negative implications for work (Keller & Alsdorf, 2012). This study attempted to highlight the valiant efforts of IS professionals fighting to defend an

organization against the frailties of human character that leaves an organization open to attack by nefarious actors, even while these defenders struggle against situational constraints and occupational stressors. By eliciting the voices of IS professionals, much was learned about the vulnerabilities experienced by IS professionals daily. In the book of 2 Corinthians, the apostle Paul shares some of his own vulnerabilities related to the pressures of his role in the church:

> I have labored and toiled and have often gone without sleep; I have known hunger and thirst and have often gone without food; I have been cold and naked. And apart from other things, there is the daily pressure on me of my anxiety for all the churches. (2 Corinthians 11:27-30, New International Version)

When faced with mounting pressures and deadlines that are so often associated with the work done by IS professionals (Messersmith, 2007), it can be difficult to maintain a positive and productive attitude as Christians are encouraged to do in Galatians 6:9, "Let us not become weary in doing good, for at the proper time we will reap a harvest if we do not give up." Just as God has supplied each of his children with unique spiritual gifts to be used to serve one another, he also supplies the strength to use these gifts for his glory (1 Peter 4:10-11). The results of this study act as gentle reminder that God's grace is enough, because his power is made perfect as it shines through the weaknesses and vulnerabilities of people (2 Corinthians 12: 9-10).

Relationship to CIS. Social engineering exploitations persist even though improvements in technology and systems now have the potential to put an end to successful cyberattacks, if the human vulnerability is minimized (Flores & Ekstedt, 2016; Applegate, 2009; Shoniregun et al., 2014; Junger et al., 2017). Because social engineers take advantage of the human tendency to trust others, businesses remain open to the risks that accompany any misplaced trust (Mouton et al., 2016; Granger, 2001). Consequently, people remain one of the

greatest security threats to an organization's assets. It is the responsibility of the IS security team to ensure the appropriate measures are taken to strengthen the parts of the company most susceptible to attack.

Goal achievement. Understanding the essence about what it means for IS professionals working to prevent social engineering vulnerabilities in U.S. businesses is significant to the field of CIS because social engineers continue to exploit human vulnerabilities, resulting in substantial consequences for businesses and customers (Ponemon Institute, 2017). Knowing what happens behind the scenes of IS departments offered insights into why social engineering vulnerabilities persist even though IS professionals have recognized the need for better training for those at risk for exploitation (Jackson, 2017). Identifying commonly held beliefs and attitudes of IS security professionals revealed mindsets that may influence the productivity of these workers towards achieving their goal of minimizing social engineering threats to business (Agbonluae et al., 2017).

Summary of the significance of the study. Most successful cybercrime attacks begin with a simple, straightforward social engineering tactic (ISTR, 2017). Email phishing tactics can easily be sent to every person across a business, and all it takes is one wrong click or one unaware, trusting employee to break down and technological defenses that have been put in place (Proof Point, 2018). Criminals are acutely aware of this vulnerability, leading them to employ even more social engineering campaigns to achieve their end goals (Lavion, 2018). If tactics are not immediately shut down, businesses of all sizes face serious and costly threats to their economic welfare, brand, and reputation (ISACA, 2016). The tenacity of cybersecurity threats has garnered the attention and support of business executives and leadership, changing the classification of security problems from an IS issue to a business issue—a critical business

issue (IDG, 2016). The task of protecting a company against the evermore-sophisticated attempts to breach enterprise defenses seems nearly impossible, making it a crucial area to examine more closely in literature.

There is power to be found in exploring and understanding the exposed areas of a business. Security professionals are placed in vulnerable positions with great pressures and expectations to keep assets secure from unauthorized users. Understanding the phenomenon of IS security professionals working to defend an organization against social engineering threats is essential because it allows those living the experience to respond to activities and directives that security professionals are expected to perform to protect the organization. Hearing the point of view of IS security professionals had the potential to expose commonly held misconceptions about what may be contributing to the failed attempts at thwarting social engineering attacks at U.S. businesses. Hearing this perspective can also help businesses learn what may be standing in the way of successfully ending social engineering attacks, so a more appropriate response may be built for addressing the situation. The findings of this phenomenological study may also lead to the development of new theories, changes to expectations or policies, or inspire action to address or challenge the issues voiced by study participants.

A Review of the Professional and Academic Literature

The review of professional and academic literatures begins with an overview of how cyberattacks affect the overall business landscape. From there, social engineering, one of the most commonly used methods used by cybercriminals to perpetrate an attack and the focus of this research effort, is explored. Following the examination of social engineering as a whole, the focus of the literature narrows down to reveal how social engineering and cyberattacks are being targeted at specific industries. After the analysis of how and why cybercriminals aim social

engineering and cyberattacks against specific industries, the scope of the literature begins to concentrate on the role of the IS professional, both overall and as a security professional defending the organization against attacks. Last, the scope of the literature review is constrained to look even more closely at the role occupational stress plays in terms of the IS professional responding to the high work demands, changes, and expectations. The review concludes with themes, perceptions, and a summary of the discoveries from the literature. The researcher designed Figure 2 below to provide a visual road map of the structure used to narrow the focus of the literature review.

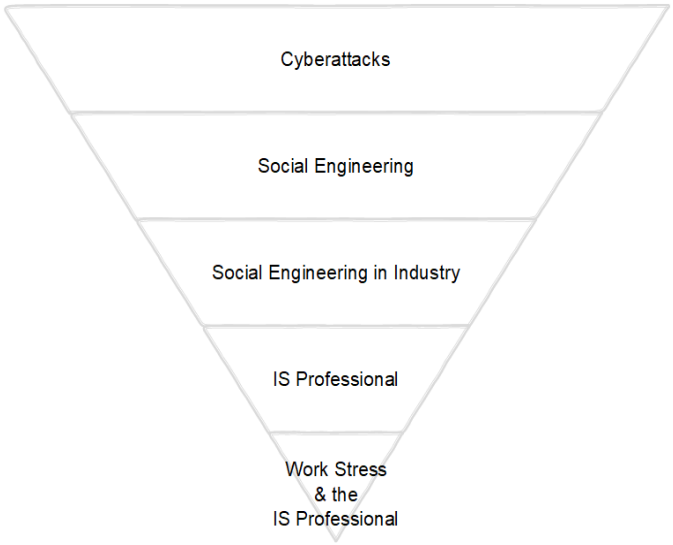

Figure 2. Literature review road map structure.

Cyberattacks. Cyberattacks are more common than ever (Amsden & Chen, 2012). In fact, Ilves (2016) posited that the more digitized a country, the more vulnerable the country is to cyberattacks. Still, digitization is the where the future leads, which makes building a powerful security information infrastructure extremely relevant. Considering the day-to-day activities that have already started to shift online in the U.S. and abroad, activities such as banking transactions, tax returns, bill pay, prescription orders, and even elections, the truth is the digital age increasingly opens opportunities for each of these systems to come under attack by malicious

actors. Furthermore, the power grid, financial markets, hospitals, traffic control systems, banks, credit cards, and any other civilian or commercial networks that utilize technology can all be targeted for an attack, which can have ruinous effects for the economy, businesses, and individuals involved. Still, Ilves (2016) reminded of the importance of recognizing that the risk does not come from the use of technology itself, rather the risks arise from the malicious, unintended use of technology.

The threat cyberattacks pose to national and organizational security have governments, executives, and IS professionals across the globe paying close attention to which organization or systems will be targeted next (Hathaway et al., 2012). Yet, even as many are on high alert, Hagel (2014) pointed out that many businesses still underestimate cyber threats. This mindset can be seen when companies do not adequately budget for and manage the budget-related information security decisions (Brown, 2018). Contributing to the underestimation of cyberattacks as a threat may be the fact that the meaning of the term cyberattack is fairly obscure (Kadivar, 2014). In fact, Hathaway et al. (2012) submitted that the absence of a shared definition for identifying incidents as a cyberattack, cybercrime, or cyber-warfare creates problems for the countries and governments attempting to come together to develop coordinated policy recommendations and coordinated action that address the cyberattack issue.

Nevertheless, even while an agreed-upon definition of cyberattack is still up for debate, the literature includes many characteristics of a cyberattack. Most attacks possess similar characteristics that can be classified into three main categories: attack intent, attack impact, and attack path. For an event to be classified as a cyberattack, Kadivar (2014) explained there must be at least two actors—the owner of the asset and an adversary. Next, there must exist assets that are targeted by the adversary. Then, some motivation for an attack, financial, political, or

otherwise, must be strong enough to make perpetrating an attack worthwhile for a criminal or criminal group. Fourth, something must impact the targeted assets, and fifth, each attack lasts for some length of time. Additionally, cyberattacks are also characterized as having an attack vector, taking advantage of some vulnerability, as well as starting at some origin and ending at a given destination.

Threat. Cyberattacks have fundamental differences from previous conflicts, in that cyberattacks operate on its own medium under its own set of rules (Libicki, 2009). Cyberattacks can occur, because every system has flaws that can be exploited by malicious actors. Cyberattacks do not attempt to force entry, more often they take advantage of existing vulnerabilities in the system to launch an attack. While some breaches may go undetected for a time (Hagel, 2014), other attacks can disrupt the operations of organizations across an entire value chain (O'Dowd, 2017). When unprecedented levels of disruption hit a company, operations can be postponed, appointments cancelled, and staff required to work extra hours while the business responds with contingency plans (O'Dowd, 2017).

It can take a while for a new normal to be established and depending on the breadth and scope of the attacked organization, the reach of a cyberattack can be enormous. Because of this, it remains critical for companies never to underestimate the severity of the threat of a cyberattack (Hagel, 2014). In truth, not only is it important to be aware of emerging cyber threats, but old threats should never be ignored either, as any threat might be reused by an adversary awaiting the opportunity to strike when a potential victim lets their guard down.

Security measures designed to protect sensitive information become more effective every day (Mouton et al., 2016). Even so, threat actors are cognizant of the methods businesses use to respond to the digitization of the overall economy (Airehrour et al., 2018). How businesses

collaborate commercially and socially, as well as how digitization of various business functions have transformed the way training, communication, and data sharing activities are conducted between employees, customers, and partners. Unfortunately, even with these transformational changes, the people of an organizations remain predisposed to manipulation by attackers (Mouton et al., 2016). Adding support to this assertion, Lineberry (2007) maintained that few companies properly address the human element related to information security, because many information security managers and administrators do not adequately understand the topic themselves. Using their understanding of the current trends used in industry, cybercriminals create opportunities to exploit weaknesses that result when businesses allow employees and other insiders to engage in online activities (Airehrour et al., 2018).

Trends. Cybercriminals are becoming more organized, which makes them even greater adversaries than ever before (Huang, Siegel, & Madnick, 2018). In some instances, the network surrounding cybercriminal activities has evolved to the point it now includes a completely integrated supply chain constructed around value-added processes. Moreover, Anderson (2017) recognized a problematic broader trend in cyberattacks, such that the cybercriminal, rarely receives consequences for perpetrating an attack. Case in point, when consumers are targeted, the company is held accountable for the breach because the consumer will often sue the organization for not protecting their information better (Anderson, 2017). Moreover, when a company is targeted for a cyberattack, again it falls to the company to bear the weight of responsibility of the situation, because law enforcement has not proven able to address the perpetrator in any meaningful way. Without a doubt, it is extremely difficult, if not impossible, to accurately identify the offender given information about the offending party is classified, government information, and because of this, businesses regularly choose not to report when a

cyberattack has occurred (Anderson, 2017). To make matters worse for businesses, even when hackers can be identified, if they hail from foreign territories, the legal system does not currently allow organizations enforceable, legal recourse.

Technology. Not only are hundreds of free, ready-to-use software easily available to attackers for use in an exploit (Indrajit, 2017), but also, demand for hacking products, tools, and services exist to the point that markets have been created to connect buyers and sellers of hacking tools and services (Ablon, Libicki, & Golay, 2014). The size and complexity of black markets is growing, making it the perfect place for financially motivated, highly organized groups to meet anonymously for nefarious purposes (Ablon et al., 2014). The anonymity of the hacker market presents both a challenge and threat to the organizations, governments, and persons attempting to operate in the digital economy.

Emerging technologies. The Internet of Things (IoT) and artificial intelligence (AI) has caught the eye of both organizations and attackers. As IoT ushers in a proliferation of smart, autonomously acting devices, companies and security professionals are becoming increasingly aware of how each new device extends the attack surface of the organization (O'Halloran, Robinson, & Brock, 2017). Understanding how the physical hardware and systems are targeted for a cyberattack requires companies to prioritize finding ways to enable efficient, yet secure workflows for each new tool brought into the mix. Furthermore, Advanced Persistent Threats, or APTs, are a growing security concern because they are designed to focus an attack on a specific target (Bere, Bhunu-Shava, Gamundani, & Nhamu, 2015). Most recently, the smart grid has entered the scene as a next-generation power system to revolutionize and improve upon the security of the traditional grid (Rana, Li, & Su, 2018). The smart grid offers greater efficiency, sustainability, security, and connectivity than the traditional grid, but it remains at risk for

malicious actors to attack it. A successful attack on power network operations can lead to serious and unprecedented technical, social, economic, and control complications.

Common-use technologies. Even with the new technologies drawing the attention of cybersecurity professionals, the regular-use technologies, such as email and messaging services also remain a primary cause for concern for businesses. Results of a study by Bakhshi, Papadaki, and Furnell (2009) revealed staff members remain susceptible to email-based socially engineering attacks. In the experiment, 152 staff members received an email requesting they follow a link to an external website to install a software update. Even though the experiment occurred during a very short window of time, 23% of those receiving the email fell for the attack. Given that all it takes is a single incident to create opportunities for an attacker to exploit an organization, results like these provide visible evidence of huge vulnerabilities of organizations to socially engineered exploits.

Technological vulnerabilities. In the modern age of cybersecurity, the offensive and defensive sides utilize comparable innovations in the race to overcome the opponent (Huang et al., 2018). Consequently, as systems advance, so do vulnerabilities that must be addressed (Rana et al., 2018). With each new technology brought in to improve some business process or function, organizations must consider each way an attacker might turn this tool against them to the detriment of the company and its stakeholders. Critical systems of a business rely on other systems, both within the organization and across the value chain (O'Halloran et al., 2017). Therefore, because cyberattacks threaten anyone and everyone, companies need to be assured that the systems their systems depend on are secure. This means as cyberattacks continue to increase in quantity and severity, privacy, security, resilience, and safety will be at the top of the

list of concerns needing to be addressed to ensure security verification and validation methods work properly.

Cost. Organizations say cybercriminal activity is the biggest threat to enterprise resiliency (ISACA, 2016). In reality, cybercriminals use internet crime schemes to pocket millions of dollars from victims each year (FBI, 2018). The enormity of the consequences of an incident on brand reputation and on finances is driving companies to address the risk (ISACA, 2016). Not only are businesses are spending a sizeable portion of the IT budget on high tech computer security (Lineberry, 2007), they have started to accept that most technical security controls are ineffective at protecting the organizational assets against many types of cyberattacks, especially social engineering attacks (Berti, 2003). Companies now recognize even if significant investments and efforts are made to improve technical security controls, but insiders remain susceptible to ploys that take advantage of human nature within the organizational context, then social engineering attacks will continue to succeed at getting around this layer of defense. Given that primary targets of social engineering include help desks, administrators, technical support staff, and other common employee positions, all employees of a business require an understanding of information security to ensure organizational assets remain protected. Designing effective training and creating a culture of security requires dedicated financial commitment by the company.

Defenses do not come cheap. There are numerous other costs associated with protecting an organization from cyberattacks, responding to attack attempts, and recovering from a successful attack. Adequately protecting organizational assets comes down to the implementation of three categories of mechanisms, including physical security, technical security, and administrative security (Berti, 2003). Even as governments and organizations

spend millions upon millions on cyber systems to improve security, sometimes cybercriminals win the day, because all it takes is finding one weak hole in the multi-million defense system to unlock access to the kingdom (O'Dowd, 2017). Therefore, investments must also be made in hiring and training highly skilled cybersecurity professionals who understands how to seek out potential security holes and put protective measures in place before a cybercriminal attempts to exploit the vulnerability (ISACA, 2016).

Hefty consequences. Of course, not every company has the budget to adequately protect itself against cyber attackers. According to Hawkins (2017), while large organizations can invest millions of dollars into cyber-security, cyberattacks can be much more devastating to the small- or medium-sized enterprises or non-governmental organizations (NGOs). Even when millions invested in cybersecurity that cannot guarantee success, as seen in the high number of recent high-profile attacks aimed at large companies across the globe. Moreover, a system can be compromised in a matter of minutes or seconds, but the company may not become aware of a successful attack until weeks or months later (Verizon, 2018). In many instances, law enforcement, a partner, or customer find out their information has been compromised before the company realizes an attack has occurred. Once the breach becomes public, situations like this can lead to a hefty blow to the reputation of the company that swiftly hurts the brand value and confidence of the consumer, putting future money of the organization at risk (Mckoy, 2015; ISACA, 2016).

Following a breach. While an attack often compromises crucial business services and put customers and their information at risk, the aftermath stemming from the breach of consumer trust is the force that can eventually compel a business to close its doors (Mckoy, 2015). State and federal laws, including HIPAA, FERPA, SOX, and PCI DCC, have been passed requiring

organizations to notify victims of a data breach to grant consumers notice and credit protection when their data has been stolen or accidentally shared with an unauthorized party (Gardner & Thomas, 2014). Not only does the company realize additional costs related to communicating the breach and providing credit protection those affected, but also, not notifying customers of a compromised data situation can results in steep fines to the compromised organization. Businesses represented in the 2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB) Keeper Security study disclosed spending an average of upwards of $1 million in the aftermath of a data breach where customer and employee information were compromised due to the IT assets that were damaged or stolen (Ponemon, 2017b). Also, the disruption to normal operations cost SMBs an average of over $1.2 million. The same study found when ransomware was used in an attack, most SMBs paid the ransom unless they had a backup, or they did not believe the services would be returned once the ransom was paid. According to the Information Systems Audit and Control Association report (ISACA, 2016), business and industry should now recognize the rate of incidence occurrences continue to intensify, making security breaches a fact of life, rather than a potential risk.

Business response. There is no shortage of research when it comes to how businesses should respond to this new 'cyberattacks are a way of life' reality. Hagel (2014) offered nine practical ways businesses can respond to improve their data security and security awareness. First, it is important never to underestimate the severity of the threat. Second, a breach can easily go undetected. Third, it is important to be aware of emerging cyber threats, but old threats should never be ignored. Any threat might be reused by an adversary. The opponent is simply waiting for an opportunity to strike when the company does not suspect an assault. Fourth, security concerns should be considered at the beginning and throughout every new project.

Fifth, leadership must be onboard and supportive of a security culture. Sixth, it is important for all employees to receive training on cybersecurity, not only the IS staff. Seventh, make sure all the technical solutions are properly implemented. Eighth, identify the most important organizational and data assets so additional security layers and protocols can be installed. Last, ask questions. More recently, the 2018 Verizon Data Breach Investigations Executive Summary report recommends businesses respond by being vigilant, making people the initial line of defense, controlling data so access is on a need-to-know basis only, patching holes without delay, encrypting confidential data, utilizing 2-factor authentication, and remembering physical security.

Security culture. Lineberry (2007) maintained if information security is to be effective, it must be culturally ingrained and supported by processes and procedures that are always being taught, tested, measured, and polished. A study by Ekwall and Rolandsson (2013) addressed the importance of establishing a security culture across an enterprise, if not across an entire supply chain. The international trading system depends on effectively transporting goods from Point A to Point B, but these transports have become more vulnerable to security threats than ever before. To increase the overall security level across the logistical chain, supply-chain security programs have started stressing the role each employee plays in reducing cargo theft across the entire supply chain. In highlighting security awareness related to specific issues, like cargo theft, the company makes an unwritten statement about its expectation of employee behavior when faced with a potential security issue. This unwritten regulation of behavior defines the company's security culture, which can help standardize the response of an employee during an unpredictable encounter with a potentially damaging security decision.

Security awareness and training. Companies investing in various ways to increase awareness about security risks throughout an enterprise. Some are attempting to find ways to use data-driven cybersecurity analytics to predict the extent a cyberattack is imminent (Zhan, Xu, & Xu, 2015). Others invest in trying to reduce the susceptibility of its people through awareness trainings and interventions (Orgill, Romney, Bailey, & Orgill, 2004). Even the most trusted employees can fall prey to moments of negligence, social pressure, and lack of awareness. One approach recommended for companies to increase security awareness and preparedness is to randomly test the human layer of security defense using surprise security audits to simulate an actual social engineering attack.

Strong policies and compliance with policies. There is no doubt that security awareness trainings are important for an organization to reduce susceptibility of human insiders to the cyber and socially engineered threats they face (Bauer et al., 2017). Still, not all security awareness programs produce the desired outcomes, making it exceedingly important for information security policies to be designed and operationalized carefully to ensure employees comply via their information security behaviors. The compliance of users with information security policies is irreplaceable if information security incidents are to be minimized. An investigation by Bauer et al. (2017) revealed that different user groups reported varied perceptions of information security risks. The study showed that some users do not consider their role important for ensuring information security and that many users did not perceive coworkers to be potential malicious actors. It was also noted that while most study participants confirmed they knew the information security policies, they typically could not cite a specific example of a single policy. Following the study analysis, the researchers proposed incorporating a full range of informational security awareness interventions throughout the security awareness program has a

greater likelihood of resulting in higher levels of behavioral compliance with information security.

Additionally, the results suggested the implementation of a long-term strategy that makes room for careful evaluation and defined control mechanisms make it likely for a company to achieve the desired level of behavioral compliance from employees. Differentiating target audiences by developing informational security awareness trainings and interventions based on the employee group and building feedback interventions into the informational security awareness programs are also expected to improve behavioral compliance. These findings were supported in the Campbell (2017) study, where participants stressed the significance of recurrent, continuous, steadfast, and personalized training to be the key to the prevention of successful social engineering attempts. In fact, respondents emphasized the importance of implementing a balanced set of both technical and behavior controls to incorporate adequate monitoring of both the technologies and people across the business.

Cybersecurity arsenal. Manske (2000) explained why it is important for organizations to understand how hackers use social engineering to the detriment of the business. Having this understanding can help organizations design controls and measures to limit its exposures to social engineering-type attacks. A study by Huang et al. (2018) identified 24 key, value-added activities in the cyber-security arena that businesses need to defend against cybercrime. The researchers propose the next step in defending against cybercriminal activities is for businesses to build an arsenal of services that specifically target specific vulnerable areas within the company. A sample of the suggested services includes Hacker Training as a Service (HTaaS), Value Evaluation as a Service (VEaaS), and Reputation as a Service (RaaS).

Controlling access. Thornburgh (2004) explained that the solution to maintaining the confidentiality, integrity, and availability of an organization's information and information system is controlling which people have access to what information. To accomplish this, a business must ensure the requestor of information can first be identified. Once identity has been verified, the requestor must demonstrate they are who they say they are. Last, the requestor must be proven to hold the appropriate credentials or clearance level to gain entry to the desired asset.

Multi-layered defenses. According to Amsden and Chen (2012), to maintain system integrity, organizations and individuals must find a way to defeat social engineering attacks through the employment of a multi-layered defense strategy that incorporates strong policies, education, awareness, and common sense. Multi-layered defense strategies are important, because if one layer of defense is penetrated, more layers exist to deny further access to the informational assets. This assertion is support in a study by Conteh and Schmick (2016). The study, designed to appraise how vulnerable an organization's information technology infrastructure was to interference, inspects the role social engineering plays in enabling network intrusions and cyber-theft. Again, multi-layered defense mechanisms are mentioned as useful to ensure if an outer layer fails, perhaps one or more inner layers can mitigate the risk, if not keep the risk from escalating into a catastrophic event for the organization. Conteh and Schmick (2016) consider security policies, technical procedures, education and training, network guidance, physical guidance, and audits and compliance to be critical to ensuring the multi-layered defenses work together to protect a business against cyberattacks.

Businesses respond through action. Less research provides evidence of how businesses are successfully responding. What has been noted is that businesses are finally concerned enough the potential fiscal damage that accompanies the risk, they are acting (ISACA, 2016).

Board members and executives are both informed and concerned, so much so that enterprises are making and enforcing stronger plans to address the ongoing cybersecurity issue. Not only are executives actively supporting security programs, they are aligning cybersecurity with enterprise objectives. Security policies are being enforced, and cybersecurity budgets are increasing so that the appropriate amount of funding is in place to support the security needs of the company. Additionally, businesses have improved system patching regimens, rolled out new security tools, and deployed layered levels of defense throughout their networks and at all end points (Proof Point, 2018). The ISACA (2016) report shows evidence that budgets are expanding to ensure skilled security workers are compensated appropriately and to support the skills development training, response planning, and awareness program needs of U.S. enterprises.

Need for defense. According to the Proof Point's 2018 Human Factor survey, perpetrators have found even the best defenses can be overcome if they can place a well-crafted email lure into the inbox of an unsuspecting insider. All it takes is a single, innocent click of an unsuspecting insider to inflict serious damages on an organization (Proof Point, 2018). In 2015, almost 60% of companies experienced a phishing attack, with almost 60% of reporting companies stating the phishing attempts happened daily (ISACA, 2016). Statistics also show that four percent of people will click on any given phishing lure (Verizon, 2018). Only making matters worse, companies also contend with insider damage and intellectual property damage on a quarterly basis. It is no wonder that not only do cybersecurity risks continue to plague enterprises, but companies expect the frequency and destructive impact of cyberattacks to increase (ISACA, 2016; IBM, 2016).

Threat actors. ISACA (2016) classifies perpetrating cyber attackers into six categories: cybercriminals, hackers, non-malicious insiders, malicious insiders, nation/state, and hacktivists.

The most frequent attacks come from cybercriminals, hackers, and non-malicious insiders. According to Verizon's 2018 Data Breach Investigations Report, study participants indicated nearly 73% of the cyberattacks came from someone outside the company. In fact, organized crime groups were responsible for half of all breaches. Still, it is insiders, or anyone trusted enough to be provided with access to business systems, who consistently give companies pause (Axelos, 2016). The 2016 IBM Cybersecurity Intelligence Index claims that insider threats pose the most significant threat to organizations, because it is more difficult to defend against someone who already has inside access to data systems and have insights into company weaknesses. Most insiders pose no danger, but it is nearly impossible for companies to discern which insider actors are an endangerment to the enterprise. In the Verizon (2018) report, insiders were involved in 28% of attacks. Sometimes the insider acted with malicious intent, but other times, they simply made costly security mistakes.

Security defense triad. Semer (2012) posited that three pieces make up the security triad: technology, processes, and people. Each piece of the triad is essential for supporting an organization's information security program. Information security research shows much emphasis placed on using technology to mitigate the threats against the organization. The employee security awareness program highlights the role of people to mitigate physical and information security threats. Processes, procedures, and audits help the company gauge whether the security awareness programs are working as intended, so adjustments may be made. Each has an important part to contribute to the effective security posture of a company.

Exploiting the unaware. Scarily, ISACA (2016) reported 24% of cybersecurity professional had no idea which group was responsible for carrying out the cyberattack on the organization, and many others reported being unaware as to whether the company had

experienced a data breach within the previous year. As the State of Cybersecurity Implications is an international survey of cybersecurity professionals, these results suggest a serious and global lack of cyber situational awareness among industry professionals that desperately needs to be addressed. Adversaries now recognize information access is not strictly limited to finding holes in an information systems' defense structure, which is growing more difficult to penetrate. Often, the easier target for cybercriminals are the unsuspecting human marks. Truly, attackers are proving highly proficient in adapting to new trends, popular interests, and usage patterns to wage attacks on the people of an organization, which make the need for fortifying defense even more relevant for business and industry. Researchers continue to seek out ways to improve informational security training and defenses against cyberattacks through the review, analysis, and critique of best practices, tactics, and techniques (Schaab, Beckers, & Pape, 2017). Still, not every countermeasure is appropriate for the type of attack strategy used, especially since some attacks, like social engineering, fall across both the technology and psychology disciplines.

Influencing attack decisions. Attackers are experts at leveraging fear and stress of unsuspecting employees to gain access to the information they seek (Spinapolice, 2011; Peltier, 2006). In an in-depth exploration of social engineering, Spinapolice (2011) found that social engineers prey on the social norms related to reciprocation, commitment, friendliness, scarcity, social proof, and authority using tactics that take advantage of the helpfulness, comfort zone, carelessness, or fear of the person being targeted. Davis (2014) argued that self-defense efforts to deter a cyberattack are rarely, if ever enough. When an adversary sizes up an identified target, they consider only a couple of courses of action, one preferable for the defender, the other undesirable. Companies can influence the decision-making process of an adversary by strengthening the perceptions of the attacker that the preferable course of action is better, or by

making the undesirable path appear even more disagreeable through the utilization of defenses known to defeat attacks or threaten punishment. Defenders must also recognize the factors that contribute to the decision of an adversary that may not be as easily influenced, such as the internal politics, rationality, nationalism or pride of the adversary. Deterrence often fails because defenders minimize the significance of these factors on the choices of the attacker (Davis, 2014).

Sharing passwords. Happ et al. (2016) revealed exactly how risky untrained and uneducated people can be to an organization's security. In a study of 1,208 participants, more than 1/3 of the participants were willing to reveal their personal passwords to a perfect stranger. Not only that, several participants provided passwords within two minutes of the interview. Another 47.4% of study participants gave numerous helpful hints to their password. In all, nearly nine out of ten people revealed some personal information to a person they were entirely unfamiliar with. In fact, analysis of the results revealed that study participants were more likely to share their password after a small incentive was received. Results of the study showed social engineering that misuses the norm of reciprocity proved successful.

Fostering a security culture. Walko (2013) suggested that not every cyberattack countermeasure needs to result in hardship for the organization, because good policies with checks in place to ensure follow-through can cover a lot of ground. According to Haber (2009), if users do not practice safe cyber practices, even installation of the latest and greatest security hardware and software cannot keep the organization safe. Still, security is not the primary job of most people working for the company, which is why the creation of a security culture across the entire enterprise is so important (Haber, 2009). Even if most will never become security experts, system users can be taught to recognize suspicious activity and provided with information about who to contact when any security-related questions come up. Small changes around the

company can foster a security-conscious culture, including displaying banners and posters in visible in physical spaces and on the company intranet. In addition, materials related to security awareness and education can be distributed at regular and irregular intervals to, or computer awareness days can be designed to reinforce training and awareness efforts, perhaps using mock security scenarios that give users hands-on opportunities to apply best practices.

Lie-detecting—an imperfect science. Because most lies are imperfectly executed, mistakes can be detected by someone trained to detect deception (Ekman, 1996). Unfortunately, the majority of people cannot tell the difference between someone who is telling the truth or lying, and even those with a trained eye can easily miss subtle changes in the body, voice or facial expressions that take place during a deception (Ekman, 1991). Because both the perpetuation and detection of lies appear to be poorly developed skills, social engineers can still successfully employ deception tactics over untrained and unsuspecting targets.

Social networks. Rather than targeting IS infrastructure, social engineering targets human vulnerabilities to gain unauthorized access to information systems (Edwards, Larson, Green, Rashid, & Baron, 2017). By employing compelling schemes, an attacker can con a mark into disclosing confidential information or interacting with malware designed to extract credentials, install viruses, or interfere with system functions until some ransom is paid. An additional area of concern for businesses is the prevalent use of social networking websites. People now reveal greater amounts of personal information on social networks, information that can be passively harvested by automated tools and placed into the hands of would-be attackers to be used to sway and influence the behaviors of identified targets.

Persisting security vulnerabilities. Many reasons contribute to the persistence of security vulnerabilities across business and industry. Many businesses confess not having the

ability to effectively mitigate cyber risks, vulnerabilities, and attacks (Ponemon, 2017b). Additionally, not only do businesses not have the ability to effectively mitigate current cyber-related issues, but they also do not feel confident of their ability to minimize the risks that arise as newer technologies, such as the IoT and AI, steadily become adopted for business purposes. From not having enough skilled security personnel to adequately manage all the security job requirements to lacking sufficient budgets for the technology and cybersecurity training needs of IS professionals and non-IS professionals alike, security issues persist for a wide array of reasons. In truth, some threats remain because even though a company might be fully aware the dangers a successful cyberattack can have, it is easier to deny the risk and assume a cybercriminal would never target them than to put appropriate defense measures in place to avoid even the most basic of incidents (Ponemon, 2017b). The next paragraphs include even more reasons security vulnerabilities persist, as found through the body of literature.

Overconfidence and lack of security skills. A study by Kessler (2016) demonstrated why social engineering threats persist despite an increase in security awareness being provided by employers. Participants in the study felt the anti-virus software, multiple authentication methods, and IT department would keep them safe from malicious activities. Additionally, the study found that participants frequently felt assured that the security controls were adequate to protect them from malicious technical attacks. They also felt confident they would be able to recognize a potential security issue, such as a phishing attempt, and that they could forward the email to the IT department to verify the identity of the sender and the legitimacy of the email. However, even with the proclaimed confidents, participants in the Kessler (2016) study failed to show actual evidence of that they truly understood what to do or how to detect a potential security issue. Unfortunately, even loyal insiders, who would never purposely aid an attack, can

inadvertently do so when their natural human curiosity, trust or desire to help someone is manipulated to give an attacker the information needed to move into the next phase of an attack.

It is easy to perpetrate an attack. One reason vulnerability persist is because it can be very difficult to spot a bad guy masquerading as a good guy. Some of the most dangerous adversaries are insiders who not only know the vulnerable places in the business, but also who usually have authorizations granting them access to the very systems and assets the company strives to protect (Axelos, 2016). The concept of information security centers on the understanding that knowledge must be available only to those who need the knowledge. It remains hidden from everyone else (Evans, 2009). To fully secure an organization, efforts must be made to find and address every single hole through which knowledge might pass through. According to Evans (2009), the attacker only needs to identify a single unsecured entry point to perpetrate a successful assault, whereas the defender must actively seek out and fortify all entry points, including those created by the people of the organization.

Security requires extra steps. Ekwall and Rolandsson (2013) reported on the dilemma faced by employees when faced with a potential security threat. While employees have required job tasks to perform on a regular basis, the occurrence of security threats is much more unpredictable. An employee faced with an unexpected potential security threat must decide to prioritize company security, which entails following additional policies and procedures, or to prioritize their normal job duties. Considering the prioritization of security tasks which will require the employee to expedite their normal duties later at a faster rate than usual to achieve the same level of productivity, employees without a cultural security compass may find themselves inclined to justify the riskier decision in exchange for maintaining current levels of productivity.

Not requiring security awareness training. Even while more businesses recognize the importance of all employees possessing an understanding about their role and responsibility in ensuring the security and integrity of systems and data, many companies still do not offer, much less require, security awareness training (Caldwell, 2016). For those companies that do offer training, great concern exists surrounding whether the training works.

Ineffective security awareness training. The compliance of users with information security policies is irreplaceable if information security incidents are to be minimized (Bauer et al., 2017). There is no doubt that security awareness trainings are important for an organization to reduce susceptibility of human insiders to the cyber and socially engineered threats they face. Yet, not all security awareness programs produce the desired outcomes. In many cases, it is questionable if awareness training is even relevant for the staff taking the training (Axelos, 2016).

Knowing-doing gap. Human insiders and system users are important in that they can either help defend the organization or they can open up additional holes in the defense to allow malicious actors a foothold. In a study by Albrechtesen (2007), a pattern indicated that users often say they are motivated to do what should be done to keep the information secure, but their behavioral follow-through frequently falls short of secure. The same study found that documented requirements of desired information security behavior and general awareness campaigns alone tend to be ineffective on influencing changes in the behavior and awareness of users. Without a doubt, user security and compliance with security policies and procedures are vital if an organization intends to hold a strong information security posture (Cox, 2012). Avoidable risks ensue when a knowing-doing gap, the gap between what information systems users know and understand and the actual behaviors they exhibit, develops. At stake, if users

engage in such risky behaviors by not following security policies and procedures, include the security and integrity of the organization, the potential exposure of sensitive information, and the weakening of the technological perimeter currently acting as a defense. Besides weakening the defense mechanisms, the reputation of the organization and any clients, partners, and customers of the organization may also be damaged by the risky behaviors--especially if these risky behaviors lead to a breach.

It is hard to spot a professional liar. Social engineers are often professional con artists who masterfully use communication techniques to get exactly what they want out of their target. Communication is based on the presumption that all participants are being truthful (Buller & Burgoon, 1996), and social engineering exploits this presupposition, to the detriment of victims. People engaged in communicative efforts engage in behaviors that Buller, Burgoon, Buslig, and Roiger (1996) classify as strategic and nonstrategic. The nonstrategic behaviors can act as indicators when deception occurs. This means, even while a deceiver attempts to project a certain image, often there are subtle clues that exist that can help recipients of a false message to know when someone is attempting to deceive them.

Security 101. Many companies still fall short on implementing a password policy, a very basic security expectation (Ponemon, 2017b). In fact, according to business representatives who responded to the Ponemon Institute's 2017 State of Cybersecurity in Small & Medium-Sized Businesses, if a company happens to have a password policy, companies do not necessarily enforce the policy very strictly. Moreover, many times companies have not implemented processes and procedures to validate whether employees are adhering to best practices in relation to password security. Indeed, many have no idea as to whether employees are using strong passwords or sharing their password with other people.

Size and risk considerations. Cybersecurity reports agree—every industry and company are at risk of being targeted for a cyberattack (Verizon, 2018; Proof Point, 2018; IBM, 2016). It matters not that a target has deep-pockets, in fact, most cybercriminals do not care who they exploit. Instead, adversaries pursue easy payouts from unprepared victims (Verizon, 2018). And, while it may require little effort for a company to convince itself they are too big, too small, or too specialized to fit the criteria a cybercriminal is looking for, no exceptions exist for those who are at risk (IBM, 2016). With the proliferation of organized cybercriminals, where bigger actors are increasing targeting smaller organizations to prey on (Proof Point, 2018), every company needs a cybersecurity strategy above and beyond the minimum level of defense to ward off potential strikes (IBM, 2016). Moreover, because cyberattacks can be so much more devastating to SMBs and NGOs, having a plan and response in place for dealing with a cyberattack is critical if the company intends to stay in business over the long haul.

Anticipatory cybersecurity. The attacks used against critical infrastructures by cybercriminals are becoming ever more sophisticated and persistent (Rege et al., 2017). To manage incidents, typically defenders await an attempt at intrusion, before responding to the attack. This response-driven approach requires significant financial resources, and it is ineffective against dynamic adversaries using adaptive approaches. The security community has started to consider how shifting to a proactive, anticipatory cybersecurity approach, an approach that adapts to adversaries at various points of the attack, might be the answer business and industry have needed all along. In learning how adversaries make dynamic decisions, a defending organization can anticipate the most effective way to keep successful attacks at bay.

Think like the enemy. Taking an anticipatory cybersecurity approach means companies need to understand how adversaries make dynamic decisions and adapt to circumstances during

an intrusion (Rege et al., 2017). For anticipatory cybersecurity measures to be designed and implemented in the enterprise setting, it is necessary for companies to completely recognize who and what they are up against (Rege, 2016). The critical infrastructures that keep a company safe from a sophisticated, targeted attack can only be properly designed if a company has captured a depth of knowledge about its adversaries. Additionally, if an organization hopes to secure itself against attacks, dedicated efforts must be made to consider potential attack scenarios from the perspective of an adversary (Evans, 2009). This anticipatory cybersecurity approach allows a company to proactively seek out and address each and every possible entry point an adversary might use to gain unauthorized access to systems.

Strengthen all weak points. Regrettably, protecting organizational assets still primarily focuses on building in the necessary technical countermeasures, even though the human component of information security continues to be crucial in successful attacks on computer systems (Mann, 2017). In most cases, hacking the people of the organization is enough for a social engineer to gather the information needed to crack into a system. Because of the human vulnerability, adversaries rarely need to seek out technical vulnerabilities to begin an attack. As adversaries continue to adapt to the trends, patterns, and interest of the mass populous, it is inevitable that a sophisticated attack will eventually take place. Hence, it remains imperative for businesses to commit to reinforcing secure practices by employees and other insiders at every opportunity. IBM (2016) offers four essential steps businesses can take to cultivate of a strategic cybersecurity program including (a) prioritize business objectives and determine the level of risk tolerance of the company; (b) protect the organization with a proactive, or anticipatory, security plan; (c) prepare a response for the inescapable sophisticated cyberattack; and (d) build, promote,

and reinforce a security awareness culture across the enterprise. Following these practices can help a company to build anticipatory cybersecurity practices throughout the enterprise.

SEDF. After consulting on social engineering assessments with many clients across varied industries without a clear-cut resource to provide guidelines for companies to reference when trying to kick off a new security awareness program, Gardner and Thomas (2014) created the social engineering defensive framework (SEDF) to help companies figure out how to stop social engineering attacks. The framework was developed after Gardner and Thomas (2014) realized that social engineering attacks could not be stopped without the right mixture of technological defense and security training. The SEDF captures their belief that building a culture of security awareness is a process, and while there may never be a cookie-cutter solution that can be implemented at every organization, by following the four basic phases outlined in the SEDF, determine exposure, evaluate defenses, educate the workforce, and streamline current technologies and policies, a company will find itself more secure with fewer vulnerabilities.

Determine exposure. In the determine exposure phase, an assessment is taken of the publicly available resources and web exposure of the company as if a social engineering were targeting the company for an attack (Gardner & Thomas, 2014). This phase should attempt to answer whether too much information is being exposed that might leave the business vulnerable to attack. Searching on information-sharing websites can reveal leaked documents among other things. The result of the research effort is a report summarizing all the information found, and the attack vectors a social engineer could use to meet with probable success.

Evaluate defenses. The evaluate defenses phase is used by the organization to take a deep look at the effectiveness each layer of defense employed by the organization (Gardner & Thomas, 2014). Typically, an organization will see how well employees resist penetration

testing and simulated attacks across various attack vectors. Detection technologies and physical security controls may be appraised to determine how well these defenses are working to protect company assets. The result of this phase can answer to what extent information or access was obtained, how many and what types of vulnerabilities left the organization exposed, whether response policies and procedures were in place and followed and more. Every answer in this phase can lead to action items that help the company fortify holes in policy, processes and procedures, attack responses, technology, and physical security.

Educate the workforce. According to Gardner and Thomas (2014), detailing each and every step in an attack scenario is critical if social engineering education is to be effective. Showcasing how metadata, phishing, social media safety, company email addresses, phone and physical attacks can be used by social engineers to launch an attack can lead to an important reality check and greater understanding for many employees. Once employees have seen how a successful attack can be perpetrated using one of these methods, it is important to follow-up with a discussion about tactics that can be used to resist leaking important information or prevent an attack.

Streamline existing technology and policy. The last phase in SEDF uses high-level scenarios designed to step security teams through an attack scenario in a non-threatening environment that supports discussions about how technological configuration changes could lead to enhanced prevention, detection, and response capabilities (Gardner & Thomas, 2014). This review walks through existing incident response policies, defensive technology, recognition competence, techniques used to lessen the impact after a successful attack and other operational plans that keep the company running in a supportive environment.

Continuous improvement. The phases in the SEDF process should be considered completely independent of each other (Gardner & Thomas, 2014). In fact, the order in which the phases are executed should align with organizational priorities at the time when the security awareness program is being initiated. Successful implementation of SEDF is seen when the discoveries from each phase result in changes to culture, training, technology, policy, or physical security measures. As SEDF is a process cycle, phases in the cycle are repeated on a periodic basis to ensure continuous improvement efforts eventually lead to a much stronger security position against adversaries.

Section synthesis. Cyberattacks are a threat to business and industry, and they usually come at a very high cost both for those who becomes victims, as well as everyone scrambling to build strong enough defenses to avoid the same fate. In truth, as the number of cyberattacks have increased, businesses have recognized the reality that preparing a response to an imminent cyberattacks is no longer an option. Instead, it is a necessity if the business hopes to keep its doors open for any amount of time. Continuous improvement processes, such as SEDF, can be used by organizations to instill as anticipatory cybersecurity culture across any size or specialized enterprise to ensure fewer any persisting security vulnerabilities are minimized

Social engineering. When considering the three pillars of the security triad (Semer, 2012), social engineering targets weaknesses in the human element of defense. Back in 1982, Rasmussen compared technology-based and human-based cyberattacks, finding human barriers much more unreliable than technical barriers. This has not changed, as can be seen in the study by Hasan et al. (2010) where the researchers had a high success rate using social engineering techniques to commit acts of deception on a Linux operating system, an operating system presumed to be the most secure operating systems around. Because the threat of social

engineering is so difficult to effectively impede, the menace of social engineering attacks continues to expand to increasingly more organizations and individuals (Amsden & Chen, 2012; Positive Technologies, 2018; Proof Point, 2018). Cybersecurity reports provide evidence that attackers now use social engineering tactics even more than automated exploits (Proof Point, 2018). In fact, cybercriminals, the most prevalent type of attacker, use social engineering more often than any other attack vector (ISACA, 2016).

Definition. Nagy et al. (2010) described social engineering as the "clever manipulation of the natural human tendency to trust with the intent to obtain information that will allow the unauthorized access to a valued system and the information that resides on that system" (p. 260). Today, the most common term in use for the person perpetrating the manipulation is *social engineer*, but in the past, people attempting to dupe others for personal gain using their wit, charm, cunning, or force were labeled grifters, con artists, and confidence men (Thornburgh, 2004). While the objectives may have changed, the manipulative tactics employed by social engineers have not. Their goal is to by-pass whatever security measures stand between them and their prize, and because social engineering attacks regularly involve person-to-person interactions that prey on the targeted individual's natural curiosity, trust, and desire to help others, they can be especially difficult for businesses to block.

An attack on human psychology. Social engineering has roots in both disciplines of computer science and social psychology (Mouton, Malan, Kimppa & Venter, 2015), but while cybersecurity professionals may be able to masterfully design and implement technical defensive tactics, many struggle to find the balance between arming the organization with the latest technological security advances and equipping company insiders with informational security skills that will assist them during a social engineering attack (Cavelty, 2014). Despite the fact

that social engineering attacks can be human-based, computer-based, or both (Maan & Sharma, 2012), at its essence, social engineering is an attack on human psychology. Neither technology or technical skills are required to commit a social engineering exploit, however, each can be used in various schemes to engage or trick an identified mark into providing sensitive information to the attacker. For example, telephone chats, phishing emails, fake mail, and POP-UP window attacks have all been used by social engineers to launch an attack on unsuspecting victims.

Social-technical system. Shozi and Modise (2015) described social engineering is a socio-technical system that recognizes the interaction between people and technology in the workplace. The social subsystem includes the people involved in the social engineering attack, specifically the victim and the attacker. The environmental subsystem is the location or medium through with an attack is perpetrated. The technical subsystem involves the technology used during the social engineering attack. Defining social engineering in this manner shows how many factors interplay with one another. Each piece of the puzzle needs to be acknowledged for the part it plays during an attack. Understanding this interplay of factors can help understand why social engineering attacks continue to be successful today.

Goal. According to Torten (2018), the primary objective of cyberattacks have not changed significantly over time. Nearly 90% of the time, financial gain and espionage are the primary motivation for an attack (Verizon, 2018b), yet, there are many other reasons companies are attacked (IBM, 2016). At times, the goal of a cyberattack is to disrupt operations, other times, they want to retrieve data, steal intellectual property, inflict physical damage, or even lodge a political protest (O'Dowd, 2017; IBM, 2016; Spinapolice, 2011). Still other times, a cybercriminal simply wishes to have a little fun—all at the expense of the target (O'Dowd, 2017).

Targets. Social engineering exploits are targeting businesses around the globe (Chitrey, Singh, & Singh, 2012), but more than anything, cybercriminals are seeking an easy target (Torten, 2018). According to Positive Technologies 2018 Cybersecurity Survey, in the vast majority of cases, the employees who coming into contact with a social engineer are not Information Systems workers. Given that primary targets of social engineering include help desks, administrators, technical support staff, and other common employee positions, all employees of a business require an understanding of information security to ensure organizational assets remain protected (Berti, 2003). Investments and efforts can be made to improve technical security controls, but if insiders remain susceptible to ploys that take advantage of human nature within the organizational context, social engineering attacks will continue to succeed at getting around this layer of defense. The literature provides insight into the various factors contributing to whether an individual is more or less likely to respond to a request made by a social engineer. Each factor influences whether the individual is a prime candidate to be targeted by a social engineer.

Individual differences. A study by Rocha Flores, Holm, Svensson, and Ericsson (2014) found that certain factors make a person more likely to respond to a social engineering ploy. Computer experience at work, gender, and the desire to be helpful were all identified as having a significant correlation with the behavior reported by respondents in a corresponding scenario-based survey. Rocha Flores et al. (2014) also discovered trust and risk behavior significant affect the actual behavior of individuals during the phishing portion of the experiment. These results suggest that techniques used by social engineers to instill trust, encourage helpfulness, and increase risky behaviors should be incorporated into security awareness training and education programs.

Personality traits. The more organizations and information security experts understand the traits of people most susceptible to engineering exploits, the more they can design interventions to target the traits that place people most at risk for exploitation and train people to use types of behaviors that protect the organizations assets from attack. Because certain human personality traits significantly contribute to the likelihood of a person succumbing to a social engineer's scam (Stewart, 2015), Workman (2007) suggested that to defend against social engineering, an understanding of human behavior is needed. For instance, in cases where social engineers target people with high normative commitment personality traits, employees may feel obligated to reciprocate social engineering gestures and favors. For example, after downloading free software, an employee may feel committed to sharing sensitive information, something they might never have considered before.

Human predictability. People possess an inherent desire to develop and maintain meaningful social relationships (Cialdini & Goldstein, 2004). They also have an intrinsic need to uphold a positive self-image. These natural motivators cause people to act or react in predictable ways to situations that appear to threaten these social needs. Someone who is aware of and skilled at manipulating this predictable pattern of behavior has the ability to use social influence processes to manipulate someone in subtle, indirect ways. In truth, after a successful social engineer exploit, often the victim is entirely unaware they have been duped into sharing information that will eventually threaten their organizational defenses.

The desire to trust. Workman (2008) found threat assessment, commitment, trust, and obedience to authority to be strong factors that, if targeted by a social engineer, enhance the chances that an attack will be successful. This is a problem, because people too easily trust others they do not know with personal, if not sensitive, information that can be used against them

in a social engineering exploit. Junger et al. (2017) used a social engineering intervention to test this theory, and found shoppers were willing to disclose their email address (79.1%), bank account information (43.5%), the type of product(s) purchased (89.8%), and the name of the online shop where the purchase transaction took place (91.4%) to someone they did not know. Even more surprising was that providing a warning did not decrease the degree of disclosure, in fact, some evidence showed a warning could potentially increase the likelihood of disclosure.

Lack of relevant security training. Results from an organizational study showed most organizations deliver some format of security awareness training, but there is no customization of the training for the distinct groups or roles across the business (Rotvold, 2007). Customization of security awareness is important helping users develop a deeper understanding of their own role and responsibility for protecting informational assets and resources (Rotvold, 2008). They must also know how they can protect information via their response to a potential security threat. Security awareness trainings that fail to prepare employees in this way leave gaping security holes in the first line of defense, holes that are easy for a social engineer to exploit.

Lack of awareness training. Demographics also contributing to type of individual targeted for a social engineering scheme. A study by Carlton (2016) established that non-IT professionals joining or leaving the workforce may be at higher risk for succumbing to a cyber-attack. In the more recent study, Junger et al. (2017) found high percentage of business schools do not offer security awareness programs, which provides additional evidence supporting the contention that new graduates entering the workforce are higher risk for the company if they are targeted by a social engineer.

Lack of security skills in practice. According to Flores and Ekstedt (2016), organizations need to establish expectations that employees are to understand security risks both in theory and in practice. To address the fact that users can still be hooked into responding to a cyberattack even with security tools embedded and working properly on systems and devices if they do not have the proper level of security awareness, Carlton (2016) designed a study to measure the cybersecurity skills of non-IT professionals. This study provides insights into which employees may be more at risk for succumbing to social engineering exploits. The analysis revealed that educational level and experience using technology resulted in significant differences between the cybersecurity skills level of non-IT professionals. In fact, higher levels of education increased the cybersecurity skills demonstrated by the non-IT professional, and the more experienced a non-IT professional was with using technology, the more likely they were to demonstrate improved skills on cybersecurity tasks.

Transformational leadership. Flores and Ekstedt (2016) also found transformational leadership to play a huge part in shaping employee attitudes. In fact, one mediation test showed the information security culture to be fully explained by the effect of transformation leadership on employee attitudes towards resisting social engineering. Even with this important insight into the role of transformational leadership on shaping attitudes, figuring out how to shape employee behavior still poses a challenge for organizations.

Success. Cybercriminals still find success using the tried and true social engineering techniques, because people continue to make the same mistakes time and again (Verizon, 2018b; Proof Point, 2018). On some occasions, social engineers launch successful largescale attacks on business and industry via blanket dispatches of ransomware and malicious phishing messages sent through email or other social network channels (Proof Point, 2018). Other occasions, the

targeted approach enables state-sponsored groups and financially motivated organized crime groups to penetrate business systems by manipulating human insiders who are highly prone to making security mistakes. Victims of targeted attacks mistakenly disclose sensitive information, click unsafe links, download insecure files, install malware, and transfer funds, all to the detriment of their employer.

Business impact. Social engineering attacks are on the rise, and when social engineering attacks are successful, they can hurt the reputation of the business, put customers and their information at risk, and even put prospective capital investment opportunities of the organization at risk (Mckoy, 2015). Sadly, sometimes the success of a social engineering attack can mean an organization eventually has to shut down operations for good. Organizations must figure out how to minimize the effects of social engineering by implementing controls that limit access to business assets until the identity and security clearance of the requestor has been verified (Thornburgh, 2004).

Social engineering tactics. Social engineers trick people into getting what they want by conveying a sense of urgency, preying on natural curiosities, copying trusted brands, and manipulating the circumstances surrounding habitual actions (Proof Point, 2018). There are two fundamental routes used by social engineers to fool a target, the direct route and the indirect route. In the direct route, a social engineer might simply ask the target for the information (Peltier, 2006). While this route may seem too obvious for someone to fall prey to, this route often proves to be effective with employees who lack basic security awareness. Social engineers also ascribe to various indirect routes that incite excitement, fear, and other strong emotions to move a target towards greater levels of susceptibility. Depending on the goal of the cybercriminal, they may employ single-stage or multiple-stage attacks (Greitzer et al., 2014).

Social engineering attack dimensions and delivery. In 2013, Tetri and Vuorinen (2013) reviewed over 40 social engineering texts to extrapolate three dimensions of a social engineering attack: persuasion, fabrication, and data gathering. According to Bere et al. (2015), social engineering is the usual means by which the delivery of Advanced Persistent Threats (APTs) in the business computer system is achieved. APTs tend to follow a six-step process that starts with choosing a victim and ends after data collection and exfiltration has been accomplished. After the target has been identified, the perpetrator builds reconnaissance, which leads to the delivery of the chosen method of attack. Furthermore, spear phishing is the number one social engineering tactic used in APTs to penetrate the security system, but other tools, such as click jacking are used at a high rate as well. Once the target successfully succumbs to the APT delivery, the attacker turns attention towards exploitation and operation. After these steps have been successfully completed, the data are collected, and removed for whatever purpose the perpetrator intended. The literature provides numerous examples where social engineering tactics are used to gain access to security-relevant data (Rößling & Müller, 2009). Descriptions of popular tactics used by social engineers follow.

Phishing. Phishing, an example of a technology-dependent social engineering tactic, uses various approaches that have grown and evolved in creativity, planning, and execution over time (Campbell, 2017). Nearly 60% of companies represented in the State of Cybersecurity Implications for 2016 report had experienced a phishing attack in 2015, and 30% experienced phishing attacks daily. These statistics are unsurprising, given phishing is the most successful social engineering tactic (Positive Technologies, 2018). Because it only takes a single person across an entire enterprise to fall for a phishing scam and four percent of people are known to click any given email lure (Verizon, 2018b), there is always a chance that a phishing campaign

will succeed (Greitzer et al., 2014). Even trained or savvy employees can be fooled, and once the social engineer has initial entry, they can enact greater misdeeds against the organization.

Business email compromise. Frequently, social engineers persuade recipients to share sensitive information or transfer money without ever having to install malware of any kind, and email unfailingly persists as the primary attack vector (Proof Point, 2018). BEC scams targeted over 400 businesses every day in the first half of 2016 alone (Symantec, 2017). Brand theft, typo-squatting, and business email compromise (BEC)-- or more simply email fraud—have proven able to fool even the savviest of users into falling for a highly sophisticated scheme. In BEC scams, cybercriminals compromise real or spoofed business email accounts using social engineering or computer incursion (FBI, 2018). BEC scams have cost companies billions of dollars in the past three years (Symantec, 2017).

Ransomware. Even more recently, cyberattacks consist of ransomware that is used by adversaries to secretly install malware to encrypt all the files on the victim's system (Krunal & Viral, 2017). It is typically used to deny the use of data or systems that are critical to the organizational operations (FBI, 2018). Once encrypted, attackers demand a ransom payment, usually in bitcoins, in return for a decryption key, which is the only way to open an encrypted file (Krunal & Viral, 2017). Even worse, ransomware has been known to cripple entire departments and organizations after only one user machine becomes infected. No longer are cybercriminals required to steal company assets to make a profit (Verizon, 2018b). Now, all they need to do is block a company's access to their data and assets using ransomware. Because ransomware is easy to install, poses minimal risk or cost, and there is no need to figure out how to profit off stolen company assets, such schemes are highly effective for cybercriminals. In fact, ransomware is now the most popular malware in use.

Social networking sites. An additional area of concern for businesses is the prevalent use of social networking websites (Edwards et al., 2017). Social networking sites allow people to reveal greater personal information that can increase the success of social engineering during an attack on its targeted organization (Mills, 2009), and attackers skillfully use social networks to their advantage (Positive Technologies, 2018). The shared information can be passively harvested by automated tools and placed into the hands of would-be attackers to be used to sway and influence the behaviors of identified targets (Edwards et al., 2017). Bolder criminals may use social networking channels to build rapport to gather information, develop a bond or send malicious links (Positive Technologies, 2018). Moreover, phishing and malware infections that harvest user credentials commonly await bargain-lovers seeking out deals social media channels (Proof Point, 2018). Because employees regularly access external and social networking sites from work sites, opening links and files received from these channels could mean a cybercriminal has access to the organization's intranet. Given these risks, employees should be diligently aware of their duty to maintain an additional level of caution during and after work hours to avoid being deceived by someone targeting their place of employment.

Social-engineering common pairings. Social engineering attacks are regularly paired with other tactics to ensure a successful outcome (Positive Technologies, 2018). In fact, phishing has been linked to malware, hacking, social media scams, fraud, ransomware, and more (Proof Point, 2018; Poneman, 2017; Verizon, 2018b; Positive Technologies, 2018). In some reports, phishing and social engineering are inextricably paired (Poneman, 2017), because pretexting, or some level of dialogue that occurs between an attacker and the victim, usually plays a role in most attacks (Verizon, 2018b). Pretexting is most commonly used for acquiring information directly from the target, whereas phishing most often centers on acquiring a foothold

within the system. According to the Verizon's 2018 Data Breach Investigation's report, malware was present in more than two-thirds of phishing attempts. Web-based attacks can work in tandem with phishing, where an email is received with a link to an external site for someone to enter their credentials. Scarily, according to Proof Point (2018), brand-registered domains are outnumbered by suspiciously registered domains 20:1, and successful phishing attempts give attackers the credentials needed to instigate the next stage of the attack (Poneman, 2017).

Section synthesis. Employees need to be aware of the benefits and risks associated with protecting computer systems as well as the various manipulative techniques employed by social engineers to trick them into making the wrong security decision (Flores & Ekstedt, 2016). Security awareness is only as useful as its ability to instill security employee behaviors that circumvent social engineering attacks, therefore once employees are aware of the security challenges faced by the organization, employees also need step up to the challenge by changing their actual security behaviors.

Social engineering in industry. While there are no industries immune to the risk of cyberattacks and social engineering (Verizon, 2018; Proof Point, 2018; IBM, 2016), some industries are more at risk than others any given year. In the Verizon's 2018 Data Breach Investigations Report, education, financial services, and healthcare are all found in the top five industries affected by social breaches, with healthcare and education in the second and third positions and financial services in the fifth position. According to Proof Point's 2018 Human Factor survey that focuses primarily on people-centered cyber threats, education was the most targeted industry for social engineering exploits. Additionally, in the 2016 IBM Cybersecurity Intelligence Index, both healthcare and financial services were included in the top three most attacked industries. Email is one of the main methods used to disrupt operations across business

and industry (Symantec, 2017). Disruptions can include spam, ransomware, or phishing campaigns, and while email malware targeted all size and type of business, the SMBs felt the brunt of the impact. This section addresses these three industries and reasons why they are currently under siege by cybercriminals.

Healthcare. Data privacy and confidentiality breaches in the healthcare industry have not relented and securing healthcare information remains one of the most difficult challenges facing people working in health-related fields (Shoniregun et al., 2010; IBM, 2016; Verizon, 2018b). With privacy and confidentiality at the heart of the need for secure systems in this field finding the best ways to protect patient information while staying in step with the latest advancements in technology has proven to be a challenge that is not easily resolved. In 2015 alone, over 100 million healthcare records were compromised, and the risks have not lessened in subsequent years (Symantec, 2017). Healthcare records fetch major returns for cybercriminals (IBM, 2017). Cybercriminals can monetize records from a successful heist and place them up for sale on the Dark Web, where they will be made available to other criminals who are interested in using the data to commit fraud, steal medical identities, or launch more targeted spear phishing exploits (IBM, 2016). Because of the amount of sensitive data contained in these files, such as social security numbers, credit card information, medical history records, the compromised data tends to stay useable for years and decades to come.

Social attacks. Phishing, pretexting, and other social attacks appear in roughly 14% of healthcare incidents (Verizon, 2018b). In healthcare, relatives and friends frequently call to find out how a patient is doing. Equipment and services providers consistently drop in and out to address issues that arise. Cunning social engineers can easily conceal the malicious intent by

contriving a similar scenario that provides them access to the system where they can gather information needed for perpetrating an attack.

Misuse and error. Healthcare is the only industry with more internal actors behind data breaches than external, primarily due to rampant errors and misuse of data and information (Verizon, 2018b). Financial gain is what motivates 40% of data breaches involving internal misuse, but other times, the internal actor is simply curious about something, so they misuse their access privileges to access informational assets without having a legitimate business or medical reason for doing so. Because of the nature of healthcare jobs, internal actors may intentionally or unintentionally share something intended for one recipient with a different recipient. This type of error, called mis-delivery, occurs in 62% of miscellaneous errors reported.

Email attacks. Like most industries, attacks that use email continue to be highly problematic for healthcare (Symantec, 2017). Email is also a means by which ransomware penetrates healthcare organizations. In fact, ransomware accounts for 85% of all malware in healthcare (Verizon, 2018b). In 2016, healthcare services noted an increase from 1 in 396 email malware incidents to 1 in 204. According to Symantic's 2017 Internet Security Threat Report, the healthcare industry was the second sub-sector in the business sector of breaches by the number of incidents.

Financial services. It makes sense if the primary objective of most cyberattack campaigns is financial gain (Verizon, 2018b; IBM, 2016), that the financial services industry would be a primary target for those seeking for a big payoff. Exploitation of vulnerabilities in the financial services sector often provides cybercriminals with the ability to read, alter, and delete confidential data (IBM, 2017). The databases of financial services organizations capture

and maintain significant quantities of personally identifiable information, the type of data that can be held for ransom or sold to the highest bidder on the Dark Web.

Trends. While financial services breaches have refined and improved monitoring and detection capabilities, breaches still exist due in part to conveniences proffered to customers such as ATM service (IBM, 2016). Finance, real estate, and insurance sectors were found to be second most likely to fall prey to a data breach, and the amount of financial information lost in data breaches increased from 2015 to 2016 (Symantec, 2017). External actors were behind 92% of data breaches that occurred in the financial and insurance industries (Verizon, 2018b). Personal, payment, and banking records were all compromised in the reported incidents. Again, email is the attack vector of choice for most cybercriminals. Social engineering attacks, especially phishing, were involved in more than half of the top category of data breach patterns, and ransomware was behind most incidents classified as crimeware.

Higher education. Of threats to the industry of education, most are perpetrated by someone outside the company (81%), but insiders also play a role in 19% of system compromising situations (Verizon, 2018b). Even though financial gain leads the motivation behind the 70% of breaches, cyber-espionage is a significant trend, accounting for 20% of breaches. This followed by 11% of breaches occurring as a result of some person looking for a bit of fun. The type of data compromised in an attack include personal data, secrets, and medical information. Educational websites were the seventh most frequently exploited across industry websites (Symantec, 2017).

Social attacks. Social incidents are one of the most common type of incident taking place across educational industries, and these types of attacks are increased (Proof Point, 2018; Verizon, 2018b). In fact, cyber-espionage, one of the top trends happening in the education

sector, is commonly used in conjunction with phishing schemes or other social engineering tactics. Because schools and universities tend to be more transparent than most other industries in regard to the disclosure of names, job titles, and other contact information for employees, more information is readily available for cybercriminals to use in a targeted attack campaign. In recent years, a prolific social engineering scenario, the W-2 scam, has become a serious issue for institutes in the education industry. The success of this scam may partially be attributed to how much information is accessible to adversaries in need of an easy target.

Section synthesis. Socially engineered cyberattacks are thriving in all industries, especially healthcare, financial services, and education. Whether an attacker uses spam, ransomware, or phishing, email is the one of the most popular and effective vectors used by cybercriminals to gain access to a system. Money is still a primary motivator behind an attack, whether the attack originates inside or outside the company. Still, attacks are successful because of errors and misuse by insiders.

IS professionals. According the 2018 U.S. Department of Labor, Bureau of Labor Statistics (BLS) Occupational Outlook Handbook (OOS), CIS professionals perform a variety of work depending on their area of specialty. Still, while positions span across computer support, database administration, software development, web development, security analysis, networking, and research, problem-solving exists as the central tenet of every position in the field of computer information systems. Because of greater emphasis on big data, cloud computing, and information security, demand for workers in this area is expected to grow faster than average for all occupations (BLS OOS, 2018). While the type of work a IS worker is eligible to enter hinges on the entry-level education necessary for the work, most require a bachelor's degree to be eligible for entry-level positions. Some jobs only require an associate degree to qualify them for

work in this field. In May 2017, the BLS OOS (2018) computed the median wage for occupations related to computer and information technology, $84,580, as higher than the median annual wage for all occupations, $37,690.

Daily work demands and expectations. The daily work demands and expectations for people working in computer and information technology occupations are high. From inventing and designing new tools or approaches, finding innovative solutions for technology that is already in use, or planning and implementing security in an effort to protect systems and networks, CIS professionals often have many projects going on at the same time (BLS OOS, 2018). The work of CIS professionals does touch on every part of an enterprise, often helping bring business and technology together to enable operations to run more efficiently and effectively.

Security workers. Security workers are responsible for planning and carrying out the security functions required to protect the computer systems, networks, and assets from exploitation by cybercriminals (BLS OOS, 2018b). Workers in this area must stay abreast of IT security trends, while also keeping a close watch on the most current attack techniques and vectors being used to penetrate computer systems. It is also typical for security workers to play an active role in the disaster recovery and response planning of the business, so appropriate preventative processes and procedures are implemented. If performed well, in event of a security crisis, business function may remain online or be restored more quickly than if no plan existed. Qualified security workers are in high demand, and their job responsibilities continue to grow as the quantity and sophistication of attacks increase. According to BLS OOS (2018), information security analyst jobs are expected to grow 28% from 2016 to 2026, a much faster rate than the average of all other occupations.

Skills and qualifications. Most employers prefer security workers to have obtained a bachelor's degree or higher in information assurance, programming, computer science or similar fields, and experience in the field is often preferred (BLS OOS, 2018b). Employers have also expressed interested in security workers possessing both business and computer expertise, as can be seen by those employers who prefer when applicants have earned a Master of Business Administration with an Information Systems concentration area. General certifications, such as the Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), CompTIA Security+ and Certified Information Systems Security Professional (CISSP), can be helpful in setting an applicant apart from others in an applicant pool. Other important qualifications security workers need to be successful include strong analytical and problem-solving skills, a detail-oriented nature, and an inventiveness that can be used to come up with creative solutions to protect the company from unauthorized network and system access.

Demand and shortage. More security positions exist than organizations can find qualified security workers to fill them with (ISACA, 2016). It often takes upwards of three months to fill a cybersecurity job opening, if the position can be filled at all. Even though budgets have improved over previous years to ensure security workers are adequately compensated for the work they perform, the pool of suitably qualified candidates is insufficient for to meet the needs of business and industry. Still, companies are so desperate for security help, they are willing to hire workers lacking in important qualifications—hands-on experience, understanding of the business, and technical and communications are often deficient at time of hire. This shortfall of employable security workers makes more frequent and more damaging data breaches possible (ISACA, 2016). The organization lacking a skilled security team hinders

its ability to identify, suppress, and alleviate security events, resulting in greater losses related to the event.

Challenges. While the biggest challenge faced by companies while attempting to enact a stronger security posture is the lack of personnel on staff to minimize the threats and vulnerabilities, there are many other issues security workers frequently contend with (Ponemon Institute, 2017b). For instance, new policy can be reason for concern for security workers, because new policies often necessitate changes to the present security strategy. At the same time, many security budgets still fall short of the necessary funding to ensure a strong security stance for the organization. Skills training is not only important for security workers to stay abreast of the latest cybersecurity skills and technologies (OOS BLS, 2018b), but also, security awareness training is extremely important to strengthen the security stance of non-IS professionals who are regularly targeted for attack by social engineers (Dahbur et al., 2017; Bauer et al., 2017; Torten et al., 2018). Additionally, those organizations that hire security workers with deficient skills often find these security workers unable to understand how they should be protecting the company (Ponemon Institute, 2018b). Other challenges faced by IS security professionals are highlighted in the following paragraphs.

Attack surfaces. The set of entry points, exit points, and data channels in a system make up the attack surface of a service (Manadhata & Wing, 2010). As more attack surfaces are used across and enterprise, it becomes exceedingly more difficult to maintain higher levels of security across all surfaces. It is very important for a company to be aware of each and every attack surface of the organization, because each attack surface must be secured if the company hopes to fortify itself against attacks.

Multi-layered defense. A study by Chitrey et al. (2012) confirmed the importance of utilizing a multi-layered approach to thwart the efforts of social engineering-based attacks. This assertion was also supported by Conteh and Schmick (2016) in a study designed to appraise how vulnerable an organization's information technology infrastructure was to interference. Conteh and Schmick (2016) explained the role social engineering plays in enabling network intrusions and cyber-theft. Again, multi-layered defense mechanisms are mentioned as useful to ensure if an outer layer fails, perhaps one or more inner layers can mitigate the risk, if not keep the risk from escalating into a catastrophic event for the organization. Conteh and Schmick (2016) consider security policies, technical procedures, education and training, network guidance, physical guidance, and audits and compliance to be critical to ensuring the multi-layered defenses work together to protect a business against cyber-attacks.

Social engineering prevention. Peltier (2006) asserted that employee awareness, cooperation, and commitment to security safeguards and controls must be the first line of defense against social engineering attacks for organizations to be impregnable during an attack. The only way to maintain this line of defense is to regularly test and raise the bar across all areas of the business. According to Nagy et al. (2010), the way to accomplish this monumental task in a world of increased information sharing is to require greater information protection and verification procedures. Measures already exist to prevent social engineering within an organization, but none fully diminish the human vulnerabilities targeted in social exploits. Nagy et al. (2010) claimed that a culture that demands verification of proper access to information prior to trusting the requestor can help to eliminate nearly all social engineering attempts.

Protection of digital assets. Enterprises deal with cyberattacks on a daily basis, and motivated adversaries are able to dynamically evolve in order to achieve their goals (ISACA,

2016). Protection of digital assets is on the list of growing concerns for businesses (Torten, 2018). A successful cyber-attack and data breach has an effect on business performance, reputation, and it can compromise intellectual property. Attackers know how to surf social networks to glean information about employees (Positive Technologies, 2018). To stay in front of the next attack, cybersecurity professionals must constantly evaluate the technologies being used by the organization and come up with and implement innovative solutions that ward off criminals who are always on the prowl, searching for the conquest of an easy target (Torten, 2018).

Cycle of cybercrime. Kshetri (2006) explored the characteristics and relationships between cybercriminals, their cybercrime victims, and law enforcement agencies. The study divulges how a lack of confidence from victims towards the capability of law enforcement agencies to address their cybercrime concerns reinforces an unfortunate cycle. Kshetri (2006) showed how the victim's weak defense mechanisms, low reporting rates, and willingness to comply with the demand of a cybercriminal increases the success and confidence of attackers, thereby encouraging cybercriminals to carry out even more exploitations of vulnerable companies in the future.

Section synthesis. Jobs in information systems fields, especially security fields, are in demand. Businesses seek to fill security positions from a limited pool of candidates, which leaves many companies at greater risk because not enough workers are available to fill the need, nor do the available workers have all the necessary qualifications to ensure the enterprise will be protected once the person is hired. The challenges faced by those working in information systems and security fields are varied and complex, and while some budgets have increased to

adequately face the security challenges of the organization, many security teams lack the funding needed to ensure a strong, multi-layered defense against cyberattacks and social engineers.

Occupational stress and the IS professional. According to Rajeswari and Anantharaman (2005), the work performed by IS professionals spans across the various departmental boundaries of a business. This means IS professionals often experience additional pressures not only to possess a strong technical background, but also to prove competencies related to interpersonal skills and organizational knowledge, all while working in a demanding work environment known for unwavering deadlines, extended work hours, and dependencies necessitating interactions with clients and team members living across varied time zones around the world (Rajeswari & Anantharaman, 2005; Lim & Teo, 1999). This unique work environment contributes to IS professionals feeling higher levels of occupational stress and work exhaustion (Shih, Jiang, Klein, & Wang, 2013). Certain occupations, including CIS occupations, tend to suffer higher rates of job burnout. Cavelty (2014) discussed the dilemma that exists between the need to align an organization with its security needs while also removing its vulnerabilities. It is not an easy task to balance the instatement of the company's technical security needs while also ensuring industry professionals are adequately armed with the information security skills, skills that may feel outside of the scope of their regular job duties, to defend the organization against cyber predators.

Factors contributing to occupational stress. Occupational stressors can be classified into organizational and individual factors (Lim & Teo, 1999). Employers often find themselves limited in their ability to control the job-related factors related to occupational stress (Armstrong, Brooks, & Riemenschneider, 2015). Still, organizational responses matter as job-related factors

play a significant role in the level of career satisfaction and work-life conflict experienced by the worker (Jiang, Huang, Klein, & Tsai, 2018; Messersmith, 2007).

Organizational factors. A factor analysis of survey responses by Lim and Teo (1999) revealed six major dimensions of stress linked to characteristics intrinsic to the work environment of the CIS professional. These dimensions include: (a) work demands, (b) career concerns, (c) role ambiguity, (d) relationships with others, (e) systems maintenance, and (f) administrative tasks. Ongori and Agolla (2008) later identified lack of empowerment, high job responsibilities, inadequate pay, work overload, staff shortages, and inadequate work resources available to perform their job duties as contributing negatively to the work experience. According to Salanova et al. (2002), high demand jobs accompanied by low job control trigger work exhaustion in technology workers. Viljoen and Rothmann (2009) found low individual commitment to a company could be predicted by work-life balance, job burnout, control, and pay.

Individual factors. Mourmant, Gallivan, and Kalika (2009) examined various job characteristics of jobs in CIS fields. The results indicated job satisfaction is more often contingent with individual motivations rather than related to the organizational circumstances. Stress is perceived differently by every individual, even among those working in similar roles (Rajeswari & Anantharaman, 2005). Confidence, self-esteem, technical competence, intrinsic motivation, and self-efficacy all factor into how well a CIS professional copes with occupation-related stress and job burnout (Fu & Chen, 2015; Colomo-Palacios, Casado-Lumbreras, Soto-Acosta, García-PeñAlvo, & Tovar-Caro, 2013; LeRouge, Nelson, & Blanton, 2006; Rajeswari & Anantharaman, 2005; Salanova et al., 2002).

Influence of occupational stress on workers. The study by Salanova et al. (2002) showed the how occupational stress caused by organizational factors can adversely affect the attitudes and job strain felt by employees. The study depicts how even if a highly competent team of workers who are confident in their ability to deal with the high demands of their job have been hired, if the work environment hinders this team of workers from producing their desired outcomes, eventually the worker will become tired, pessimistic, and give up. Occupational stress has consequences for the attitudes, beliefs, motivations, and behavioral intentions of employees (Flores & Ekstedt, 2016; Cox, 2012), and beliefs, attitudes, and behavioral intentions affect individual behavior (Fishbein & Ajzen, 1975).

Attitudes and behavioral intention. The Cox (2012) study is important because it establishes the existence of a link between organizational policies, attitudes, compliance behaviors, and the resultant business risks. In the study, information system user attitudes are examined for their role and intention towards following information security policies and procedures. The findings supported the role of perceived vulnerability, subjective norms and self-efficacy as significant contributors to whether a user followed corporate security policies and procedures. The insights gained from examining the link between user security attitudes, risky behaviors, and heightened security risks provide support for the need for a similar study to examine and understand the attitudes and behaviors of IS professionals attempting to defend an organization from cyber-attacks, including social engineering attacks, as attitudes often contribute to the behaviors displayed by an individual.

Attitude and intent to resist social engineering. Flores and Ekstedt (2016) conducted an empirical study of nearly 4,300 employees to investigate how organizational and individual factors interact to complement one another when it comes to shaping employee intent to resist

social engineering. The study revealed that attitudes make a difference in intent and subsequently behavior—more so than self-efficacy and normative beliefs. The results indicated that the attitude of the individual towards resisting social engineering has the strongest direct association with the intent of the individual to resist social engineering attacks. Both self-efficacy and normative beliefs were revealed to have a weak relationship with the intent to resist social engineering. The results of the study indicate that both attitude and normative beliefs play a part in directing the relationship between information security culture and the intent of employees to resist social engineering.

Beliefs and motivations. Tarallo (2015) claimed there is no truly effective way to absolutely protect against a social engineering attack. Moreover, Davis (2014) asserted that self-defense efforts to deter a cyber-attack are rarely, if ever enough. A majority of respondents to the 2016 State of Cybersecurity survey do not believe their information security staff are prepared to address more than the simplest security events. In the same survey, most respondents confirmed a security awareness program existed at their organization, but not nearly as many believed the program to be effective. Perceptions and beliefs matter—both to IS professionals and the organizations they defend from cyberattacks and social engineering exploits. Beliefs do not negate the importance of reducing the likelihood of a successful exploit, which is the primary function of an information security team (Tarallo, 2015). Though, they can significantly influence how motivated the team is to come up with creative solutions for achieving their objective, because, as Moore (2000) pointed out, when workers perceive the causes contributing to their high levels of occupational stress and work exhaustion can be controlled, they are willing to act, speak up, or change their own behaviors to address their situation.

Consequences of work exhaustion. Work exhaustion has been linked to adverse consequences for both the individual and the organization. Greater levels of job strain have been linked to compromised health, lowered quality of life at work and at home, as well as psychological distress and cardiovascular disease for individual workers (Moen et al., 2016; Karasek & Theorell, 1990; Johnson & Hall, 1988). Organizations also suffer when workers are stressed, as work exhaustion leads to poor job performance, absenteeism, diminished work quality, and worker turnover, which can often beget the desire of the professional to leave the job or the company (Chilton, Hardgrave, & Armstrong, 2010; Viljoen & Rothmann, 2009; Lim & Teo, 1999). Different researchers offer varied solutions to how best to contend with the existence of stressors in CIS fields. Agbonluae et al. (2017) argued the importance of individual employees learning to manage occupational stress, while Moen et al. (2016) provided evidence that organizations can adequately adjust work conditions that improve well-being and reduce stress, even for technology-centric jobs. Chilton et al. (2010) supported the idea of improving individual performance by reducing job strain through actively seeking the optimal balance, or job-fit, for the IS professional's needs.

Section synthesis. The job demands of IS professionals and security professionals are high. The field of CIS is in a constant state of change, which requires workers to respond to change frequently. Every individual has a personalized response to the stress these changes invoke. Some workers respond well, while others do not—and even though one worker responds well to one change, they may not respond well to another. Occupational stress can lead to job burnout, which can have undesirable consequences for both workers and the organization. Still, ways exist for workers to learn to cope, organizations to modify working conditions to improve

worker well-being, and for organizations and employees to work together to find the right job-fit that optimally balances the needs of both the organization and employees.

Themes and perceptions. Woven throughout the body of literature can be found three themes: evolution, skill, and consequences. Each of these themes may stand alone. They may also be seen interacting with the other themes to tell the story of the interplay between social engineering, IS professionals, and the defense against cyberattacks.

Evolution. The first theme found across the literature is the theme of evolution. The field of CIS is marked by constant and ever-changing trends and patterns. Evolving technology often requires making changes to the current methods of conducting business. From changing policies, standards, and practices, advances in technologies require IS professionals to modify tactics used defend the company. As the world of business has become more digitized, the types of attacks used by cybercriminals have evolved to take advantage of security holes created by digitization. The innovative and dynamic practices of cybercriminals have forced IS professionals to develop new ways of thinking about how to protect the company. This constant state of change and evolution produces different responses for different workers, and both organizations and IS professionals have been forced to evolve in how they perceive, plan for, address, and cope with the occupational stressors that accompany this constant state of change.

Skill. A level of skill is expected of people working in IS professionals, especially in the area of information security. It is no small task to balance the high work demands that come with the job of defending an organization from cyberattacks. IS workers often find a need to develop both a specialized technical skillset as well as a broader set of business skills such as communication and interpersonal skills. It is probably not a surprise that people possessing this unique combination of technical and business skills are lacking, making them a precious, high

demand commodity. Perceptions about one's skill level can affect beliefs, motivations, and behavioral intent, which contribute to the performance and behaviors taken by employees. Cybercriminals and social engineers are masterminds in their own right, as it takes a level of sophistication first to identify areas of weakness, and then to use this knowledge to successfully pull off a complex, multi-dimensional scam.

Consequences. Every security action taken or not taken by a company results in a stronger or weaker security stance. The company that fails to think of every new trend or technology as a potential security threat, leaves themselves open to serious potential losses resulting from a successful data breach, but those who stay abreast of the challenges in the industry can develop an anticipatory cybersecurity stance. Not providing adequate training for security professionals or non-IS professionals ensures gaping holes will persist in the company's defense against cyber threats, whereas budgeting for the appropriate levels of security training can lead to a security culture across the enterprise. Last, not considering how excessive work demands may be harming IS staff also hurts the company when occupational stress leads to lower performance, absence, diminished work quality, and eventually turnover in the on the IS team. Treating IS staff as business assets to be protected and prioritized in terms of their well-being can improve job satisfaction and employee retention in positions that are difficult to fill with skilled human capital.

Summary of the literature review. The review of the literature begins with the introduction of a current problem faced across the business landscape, cyberattacks. The growing presence of cyberattacks on business and industry has added complexity to the role of IS professionals in business, a complexity that cannot be ignored without peril. Cybercriminals, at their core, are people trying to take advantage of others for personal gain. While the

motivations behind an attack are as old as time, generally avarice, the digitization of the economy has ushered in technologies that have upped the ante in terms of the methods needed to launch a successful strike. Still, cybercriminals are rising to the challenge, banding together, and becoming more dangerous with each successful criminal endeavor.

Because most cybercriminals seek the biggest payoff for the least amount of effort, any and every company can be targeted. This means SMBs, those without deep pockets that cannot afford the same security precautions as their larger counterparts, must diligently seek innovative, yet effective solutions to ensure they are less susceptible to the threat of a cyberattack. Any company refusing to acknowledge the risk or to follow through with investments in cybersecurity technology, teams, policies, procedures, training, and behavioral monitoring set themselves up for significant damages that may come in the form of a service disruption, data breach, theft of company secrets, or the loss of customer trust, brand reputation, and future business.

Company defenses are made up of physical, technological, and human barriers. The human layer of defense is consistently less reliable than technical barriers, which makes it an easier target for cybercriminals to target. Social engineering one means by which cybercriminals manipulate someone into giving them what they are after, and a successful social engineering scheme often means bad news for the unsuspecting target. Social engineering is used more often than other attack vectors to breach the human layer of defense, and it is also used in conjunction with other attack vectors like malware, hacking, fraud, ransomware, or social media scams. Common social engineering tactics include phishing, ransomware, phone conversations, and business email compromise.

Cybercriminals target personality traits, human predictability, and the desire to trust and engage with others, all to gain unauthorized access to company assets. If a company has not provided the necessary security awareness and skills development training, people will continue to succumb to the same ploys they have frequently fallen for time and again. Cybercriminals also target specific industries more than others. Consistently in the sights of attackers are healthcare, financial services, and education industries, because the value of the data and information maintained on their customers can produce a sizeable payoff on the black market.

The IS team tasked with defending the organization against cyberattacks and social engineering exploits are busy people, and often security is just one more thing on the long list of activities they must keep up with. As the cyber threat has increased, so has the need for qualified security workers, and there simply are not enough trained workers to fill the job openings. Still, while the lack of skilled security personnel has created the greatest challenge for business and industry, this is not the only security challenge, much less business challenge, IS professionals must overcome. Indeed, attack surfaces are growing, digital assets must be protected, all aspects of the security strategy of the company must be in alignment, and a security cultures must be cultivated.

Responding to the constant change, pressures to prevent security threats, tight deadlines, and extended work hours takes its toll on IS professionals, especially when many security workers have been hired while they are still underqualified and inexperienced. Some of the factors contributing to occupational stress can be influenced by the organization. Other factors take place at the individual level, but it is the combination of factors contributes to the level worker exhaustion and the subsequent, adverse effects on the individual and the organization. In sum, the review of the academic literature has yet to explore what the experience is like for IS

professionals working such conditions and what these experiences mean for their ability to produce the level of defense required by the ever-threatening landscape in which they operate. This study attempts to address this deficiency in the literature.

Transition and Summary of Section 1

Thus, concludes Section 1, the Foundation of the Study, in which the background of the problem, problem statement, purpose statement, nature of the study, research questions, conceptual framework, definitions of important terms, assumptions, limitations, delimitations, the significance of the study, and a review of the professional and academic literature were examined in great detail. As discussed, U.S. businesses remain vulnerable to costly social engineering attacks, even with technological advances that deter malware and hacking attempts. Yet, if a social engineer can hack the human to compromise the credentials of a single individual, any business investment made to strengthen technological barriers becomes worthless. The body of literature covers the cost of a successful cyberattacks to business and industry, information about how businesses are targeted, the significance of security awareness and training to help prevent attacks, and the role of the IS professional in defending the organization from social engineering and cyberattacks. Still, social engineering attacks persist, primarily because they are so often met with success, which can be as lucrative for the attacker as it is costly for the business.

The body of literature indicates that the typical working environment for the IS professional tends to be made up of many factors that inevitably lead to occupational stress. Given the role of occupational stress on worker attitudes and behaviors, questions remain about how the levels of occupational stress experienced by IS professionals may come into play in terms of the quality and quantity of anticipatory cyber defense tactics employed across an

enterprise. It is not unusual for cybersecurity reports and research studies to direct IS professionals and businesses the many techniques they should be using to protect their organization from social engineering and other cyber threats, but hardly any studies give cybersecurity professionals the opportunity to respond about what may be taking place behind the scenes to hinder their efforts. Even though the primary purpose of the study was to investigate how IS professionals working in U.S. businesses make sense of their lives and experiences while trying to prevent social engineering attacks, the study also (a) presented an opportunity for IS professionals to respond to the expectations placed upon them and (b) gave voice to the realities experienced by IS professionals on a day-to-day basis that may be influencing their ability to successfully do their jobs. This study utilized a transcendental, phenomenological qualitative research design to fill the gap in the literature. The study now transitions into Section 2, the Project, where the investigation into phenomenon of IS professionals protecting U.S. businesses from social engineering attacks begins.

Section 2: The Project

Section 2 describes the transcendental qualitative, phenomenological approach used for this study. This section begins with a review of the purpose of the study and the background of the problem to help readers recognize why understanding the phenomenon of people working to defend businesses against social engineering attacks was an important and relevant issue to be addressed. Next, the section details the central role of the researcher as it relates to the data collection, analysis, and reporting activities during the study. After that, a description of characteristics, constraints, and protections for study participants is provided, with additional details included about how participants were identified and invited to participate in the study. The section then outlines how the chosen research method and design were addressed to ensure the overall aim of the research effort was achieved. From there, the targeted population and sample size and its appropriateness for informing the current study is described. After providing insight into the targeted population, the data collection process is illustrated, presenting details related to how interviews with participants were conducted, audio-recorded, transcribed, and coded to address the lived and common experiences of the study participants in relation to the phenomenon of preventing social engineering vulnerabilities in U.S. businesses. The section also demarcates how reliability and validity were addressed throughout the duration of the project.

Purpose Statement

The purpose of this transcendental phenomenological qualitative study was to investigate how IS professionals working in U.S. businesses make sense of their lives and experiences as they address and prevent vulnerabilities to social engineering attacks. This larger problem was explored through an in-depth study of social engineering and its effect on IS professionals

working in U.S. businesses operating within healthcare, financial services, and educational industries across the central and northwest regions of Louisiana.

Problem background. U.S. businesses, even those with strong control measures in place, remain vulnerable to social engineering attacks (Mouton et al., 2016; Granger, 2001). Because successfully perpetrated cyberattacks can results in big payoffs, cyber criminals are always on the lookout for easy targets (Torten, 2018). Consequently, it has become vital for businesses to proactively seek out vulnerabilities and understand why they persist and how to prepare for an attack (Lavion, 2018). This study was designed to help businesses better understand the phenomenon of IS professionals as they defend the company against social engineering attacks, thus enabling them to develop a deeper comprehension about what continues to impede progress on the security front within this domain.

Role of the Researcher

In all research studies, initially, the researcher is responsible for laying out the foundation of the study and answering any questions surrounding the basic characteristics of the study (Creswell, 2014). This process may include providing adequate details about what the study is about, why the study is significant. The process should also cover which methods will be used to perform the study. For example, the current study utilizes a qualitative research design to investigate how IS professionals working in U.S. businesses make sense of their lives and experiences while addressing and preventing the vulnerabilities related to social engineering attacks at their place of employment. Qualitative research procedures are characterized by a holistic orientation towards exploration, description, and explanations (Krathwohl, 2009; Stake, 2010), and the researcher plays an integral role to ensure the complexities of the phenomenon under investigation are accurately captured and portrayed in such a way the remains true to the

study participant (Stake, 2010). This section describes the various roles the researcher was responsible for in the current study. These roles include designing the study, protecting the study and its participants, collecting and maintaining data, and analyzing, interpreting, and reporting the findings.

Designing the study. In addition to providing answers to the foundational questions that form the basis of the study, the researcher's role also involved designing the study (Stake, 2010). This step consisted of the formulation, planning, organization, and implementation of the step-by-step processes, procedures and time schedule to be adhered to throughout the course of the study. Stake (2010) explained that during the design process, the researcher's role is to determine which data collection techniques, such as interviews, observation, or journaling, are appropriate to achieve the purpose of the study. Interviews are a popular and useful data collection technique to achieve the desired study outcome for many qualitative research designs, especially for phenomenological research studies (Creswell & Poth, 2018; Stake, 2010; van Manen, 2016a). Once the data collection techniques are chosen, the researcher's role includes developing criteria for research participants and making decisions about whether interviews should be conducted with individuals, groups, or persons with expert knowledge and specific experiences (Magnusson & Marecek, 2015). The researcher was also required to identify the best way to conduct the interview (e.g., face-to-face, email, telephone, web conference, etc.) and to define how much data needed to be collected to sufficiently answer the questions under investigation (Fusch & Ness, 2015).

Protecting the study and participants. A very important role of the researcher in this study was to protect the integrity and validity of the study, while also safeguarding study participants throughout the research process. This study was determined to require a

transcendental phenomenology design, which presents the experiences of study participants rather than the interpretations of the researcher (Moustakas, 1994). As such, the role of the researcher was that of an outsider looking in. Accordingly, to protect the integrity of the study, the researcher was responsible for identifying and bracketing out researcher bias and underlying assumptions that can affect the study findings (Creswell & Poth, 2018). Once personal biases were extricated, the researcher identified study participants and invited them to join the study, taking measures to ensure all were willing and eligible to participate. Additionally, the researcher was responsible for preparing the interview guide and conducting the interview in such a way that (a) answered the research questions; (b) elicited open-ended, honest, robust, thoughtful responses from participants; and (c) ensured participants felt safe sharing personal thoughts and feelings (Magnusson & Marecek, 2015). To safeguard study participants, the researcher guaranteed the anonymity of participants and their employing organizations and the confidentiality of data (Krathwohl, 2009).

Collecting and maintaining data. More so than quantitative research, qualitative research requires that the researcher play an active role in the research process, as the researcher virtually acts as the primary data collection instrument (Stake, 2010; Lincoln & Denzin, 1998). In this study, the researcher's role was to interview participants, record, transcribe, and check the interview, and capture and report on relevant context occurring during the interview process. It was also imperative to capture and report on relevant contextual clues, such as behaviors, impressions and nonverbal signaling (Sutton & Austin, 2015), therefore the researcher's role also included taking field notes and keeping track of elements that cannot easily be captured from voice recordings. Qualitative research often produces a significant amount of data to keep track of (Demchenko, Zhao, Grosso, Wibisono, & De Laat, 2012), and the researcher was responsible

for creating and following a system that allowed her to collect, store, organize, and maintain data throughout the course of the study and to properly dispose of the data once the study concludes.

Analyzing, interpreting, and reporting the findings. In a transcendental phenomenological research study, the researcher also had a responsibility to hear the various voices of study participants and to produce a true, representative interpretation of the essence and shared experience (Moustakas, 1994; van Manen, 2016a). To accomplish this task, the researcher developed a coding process and used this coding process to link and connect responses of study participants (Sutton & Austin, 2015). Then, the researcher identified themes across interview transcripts until data saturation was reached. Once themes were drawn, the role of the researcher shifted to verifying the extent the findings are generalizable, reliable, and valid to ensure the intent of the research effort accomplished what it intended to accomplish. After verifying the findings of the report, the researcher synthesized these findings and presented the findings by writing the report (Sutton & Austin, 2015). To ensure the findings were representative of the true meaning that participants ascribe, the researcher was responsible for supporting any report conclusions with references to actual quotations from study participants.

Participants

To ensure the purpose of the research is accomplished, study participants must have been IS professionals with experience dealing with social engineering threats. Consequently, selected research participants were be employed as information systems professionals at organizations that have faced the threat of social engineering attacks within the previous year. No limitations were placed on the job function, age, gender, race or ethnicity of the IS professional. Rather, the identified participants had been employed by their respective organization for a minimum of one year to ensure sufficient exposure to the company culture, technologies, training, policies and

procedures. Additionally, participants were required to possess an awareness of the social engineering threats faced by the employing organization or specific experiences related to defending the organization against social engineering threats. The participants in the study were purposefully selected using professional contacts solicited within the central and northwest regions of Louisiana. As a faculty member of an undergraduate computing program at a university operating within the designated region, the researcher had access to a list of professional contacts who (a) offer insights into current industry trends and expectations for graduates of the computing program, (b) employ current students, or (c) hire graduates from the program.

Identification process. Initially, the researcher identified any contacts on this list working as IS professionals. Next, the researcher extricated which IS professionals on this list are employed by organizations operating within financial, healthcare, and education sectors. Employing organizations could be profit or non-profit entities. Once the list of potential participants was narrowed down to only IS professionals working in the designated industries, the researcher initiated contact via (a) phone, (b) email correspondence, (c), and/or (d) social media messaging services to invite them to participate in the study.

Additional leads/recommendations. Once the interviews were underway, the researcher ask study participants if they have additional contacts working within the three selected industries that might be willing to participate in the study as well, until saturation had been attained. Additionally, the researcher also explored opportunities with colleagues, friends, and family that work in the identified industries to determine whether they have contacts that could participate. The researcher accepted and followed-up on any contact information provided

by these sources to determine the willingness and eligibility to participate of recommended study participants.

Establishing a working relationship. To establish a working relationship, the researcher contacted each identified candidate via phone, email, or social media (LinkedIn or Facebook) messaging services to invite him or her to participate in the study. During the initial contact, the researcher introduced herself and the overall purpose of the research study to the identified candidate. The researcher then requested permission to follow-up with a more detailed email that officially invited the participant to participate in the study and requested responses to establish whether a participant met all the criteria to be eligible to participate in the study. For those candidates identified through snowball sampling, the researcher contacted candidates via the contact information/method provided by the reference.

A detailed email described the study to the participant and requested a response to help the researcher establish whether a participant met all the criteria to be eligible to participate in the study. The email survey asked (a) if the participant is an IS professional who works in the healthcare, financial services, or education industry and has worked in their current role for at least a year; (b) if they have experienced social engineering threats and/or attacks at their company; and (c) if they are 18 years old or older. Participants were asked to reply to the message with a 'Yes' or 'No' response to each of the questions, and they were only allowed to participate in the study if they answered 'Yes' to all criteria. The candidates were asked to respond to the email within one week. When candidates agreed to participate in the study, the researcher worked closely with the newly established participant to schedule a time and location to conduct the interview.

Measures for ethical protection. The researcher followed Institutional Review Board (IRB) policies and procedures established by Liberty University to ensure participant involvement in the study was protected. Throughout the study, candidates, and subsequently participants, were assured that any identifying information about the participant and their employing organization will not be disclosed. The researcher limited the data collected about the participant to only the information necessary to complete the goal of the study. While the researcher established eligibility to participate based on their job role, experience, industry, and region, no additional identifying information or contact information was collected, maintained, or reported. Moreover, during the interview and audio-recording process, the researcher neither solicited nor purposefully recorded the name of the participant or the name of the participant's employer. To ensure confidentiality was maintained, any identifying information was be stripped from the transcript and final report and replaced with pseudonyms or non-identifying terminology.

Concluding the study. At conclusion of the research effort, the researcher followed all protocols established by the IRB related to record retention and data destruction to ensure participants are exposed to the least amount of risk possible. Any data or records that the researcher was required to hold onto were maintained on password-protected jump drive and stored in a safe location only accessible by the researcher. Any hard copies containing identifying information will be shredded and recycled, and records will be maintained documenting when files and records were destroyed.

Research Method and Design

Together, the problem, purpose, research questions, conceptual framework, and body of literature provided the structure to support and drive the selection of an appropriate methodology

and design for this study. Each played an important role in guiding the researcher to the selection of the most appropriate methodology and design for the current study. This section discusses why a transcendental, phenomenological qualitative study was the apt choice to address the problem and purpose of the current study.

Discussion of method. According to Krathwohl (2009), qualitative methods provide researchers with a way to examine complex phenomenon that have not yet been studied before or where little knowledge currently exists about all the interwoven, multifarious parts of the phenomenon. The problem of the current study dealt with a phenomenon in which not all the variables and patterns are quantifiable, which makes a quantitative research method insufficient for addressing the needs of the study (Moustakas, 1994). Although a significant amount of effort goes into sharing important factual statistics and quantitative data about what IS professionals in annual cybersecurity reports each year (IBM, 2016, 2017; Proof Point, 2018; Verizon, 2018b; Symantec, 2017; ISACA, 2016; Ponemon Institute, 2018b), protecting enterprises from social engineering threats and other cyberattacks is a complicated issue that businesses and IS professionals do not yet have a handle on due to the high number of attack surfaces (Manadhata & Wing, 2010), need for security training (OOS BLS, 2018b), the targeting and exploitation of non-IS personnel (Dahbur et al., 2017; Bauer et al., 2017; Torten et al., 2018), and the limited number of trained security personnel available to fend off an attack (Ponemon Institute, 2017b). Additionally, while these annual quantitative reports may be extremely useful in helping researchers and IS professionals quantify how widespread and systemic an issue is being faced by businesses across the U.S. and to prioritize resources to address the issue internally, such quantitative reports cannot fully capture the essence of the experience of working daily to defend against these attacks, which is important to understand if businesses ever hope to diminish

vulnerabilities related to social engineering threats and cyberattacks (Creswell, 2014; Stake, 2010). A qualitative research method, on the other hand, can be used to understand and explore the meaning people ascribe to some situation or problem, hence justifying the need to use a qualitative method to address the requirements of this study (Krathwohl, 2009; Stake, 2010; Creswell, 2014).

Discussion of design. An assortment of qualitative designs exists, including narrative, ethnography, grounded theory, case study, and phenomenology. Because understanding the shared, lived experiences of IS professionals in preventing social engineering vulnerabilities in U.S. businesses was essential to satisfying the aim of this research effort, phenomenology was deemed the most appropriate design for the study. Moustakas (1994) explained that the purpose of phenomenological research is "to determine what an experience means for the persons who have had the experiences and are able to provide a comprehensive description of it" (p. 13). Phenomenological studies have a specific structure that is devised to produce genuine, reliable descriptions from study participants (Moustakas, 1994; van Manen, 2016a). Furthermore, phenomenology is often used to give voice to persons who have experienced a phenomenon firsthand, which in turn can provide a deeper understanding of some unique circumstance or event as it has been experienced by numerous persons (Creswell & Poth, 2018). Again, even though annual reports continuously provide relevant statistics related to the status of cyberattacks and social engineering threats in industry (IBM, 2016, 2017; Proof Point, 2018; Verizon, 2018b; Symantec, 2017; ISACA, 2016; Ponemon Institute, 2018b), as of this writing hardly any research efforts utilized a phenomenological approach to explore the shared meaning of IS professionals working to prevent social engineering vulnerabilities in U.S. businesses (Jackson, 2017). Decision-makers and policymakers, both internal and external to the company, stand to benefit

and make more informed decisions when they become more knowledgeable about common experiences of the studied groups.

Transcendental phenomenology. Because the purpose of the study was to investigate how IS professionals make sense of their lives and experiences, it was important for the study to focus more on what study participants revealed and less on how the researcher perceived the experience. Accordingly, within the phenomenological design, the transcendental approach was considered most relevant to the current research effort because of its ability to exhibit the experiences of the study participants more than researcher interpretations (Moustakas, 1994). Creswell and Poth (2018) provided a narrative of the specific procedures that researchers should follow when utilizing a transcendental approach to phenomenology. Initially, the transcendental approach requires the researcher to bracket out personal experiences, biases, and gain fresh insights and perspectives from study participants about the investigated phenomenon (Creswell & Poth, 2018; Moustakas, 1994). Once the researcher has bracketed out personal experiences, the researcher must collect data from persons who have experienced the identified phenomenon (Creswell & Poth, 2018). Next, the information collected from study participants should be reduced to significant statements. These significant statements are then analyzed and combined into themes. From here, the researcher generates a textural depiction about what participants experienced as well as a structural account of how the phenomenon was experienced, making sure to include information about the conditions, situations, and context, as described by study participants. The final procedure occurs when the researcher attempts to convey the overall essence of the experience by combining the textural and structural descriptions together, resulting in a rich detailed account of the phenomenon, as experienced by the study participants (Creswell & Poth, 2018).

Summary of research method and design. This research effort centered on producing a greater depth of understanding about an identified phenomenon, a key feature of qualitative research methods (Stake, 2010). Qualitative research methods allow investigators the ability to observe the mundane, everyday experiences of people and produce meaning and insights that can be shared with relevant stakeholders, often enabling stakeholders to make better decisions and policies (Creswell & Poth, 2018). The purpose of this study was to develop a greater depth of understanding about the common experiences of IS professionals dealing with the phenomenon of preventing social engineering vulnerabilities in U.S. businesses. Only the phenomenological research design was built to meet this need precisely, and the transcendental approach provided the structure to ensure the overall aim of the research effort is achieved (Moustakas, 1994; Creswell & Poth, 2018; van Manen, 2016a). For these reasons, the researcher deemed the transcendental, phenomenological qualitative research methodology and design the most fitting to address both the problem and purpose of this study.

Population and Sampling

The initial population investigated in this study included three IS professionals working to defend their respective organization against social engineering attacks. Participants were selected from the region and business sectors identified as important to this study. Purposive sampling, often used in qualitative research to select individuals who are able to inform the research about the selected phenomenon of preventing social engineering vulnerabilities in U.S. businesses (Krathwohl, 2009; Creswell & Poth, 2018), was utilized in conjunction with snowball sampling to select participants who were able to inform the research about the selected phenomenon (Krathwohl, 2009; Creswell & Poth, 2018). The subsequent paragraphs outline the rationale behind the chosen population and sampling for this research effort.

Population. In phenomenological research, it is important for the population to be representative of the group being studied (Krathwohl, 2009). The target population in this study focuses on IS professionals working in U.S. businesses in the central and northwest regions of Louisiana. Specifically, the targeted population were presently working in in healthcare, financial services, and education industries, because these sectors are regularly targeted by social engineers (Proof Point, 2018; Medlin, Cazier, & Foulk, 2008; Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005). Since it was important for participants to speak about their experiences involving the phenomenon (Krathwohl, 2009), it was also important for employees to have relevant experience working in an information systems related role for a period and an awareness of the phenomenon of defending the organization against social engineering attacks. Without such experience, the selected participants could not have adequately informed the study. Understanding the corporate culture and the issues and challenges related to information systems in the workplace takes time (Gamble, Peteraf, & Thompson, 2015; Mello, 2015). Consequently, to ensure adequate exposure to an employing organization's culture, policies, and IS-related roles and functions, study participants must have been employed by their respective organization in an IS role for a minimum of one year. Study participants were also required to be aware of the phenomenon of defending the organization against engineering attacks.

Persons under 18 years of age, non-IS professionals, and IS professionals with less than one year of experience working at their employer were excluded from the study. Persons working outside the healthcare, financial services, and educational sectors were also excluded. Lastly, persons with no experiences preventing social engineering at their place of employment were not eligible for participation in the study.

Sampling. Sampling, in many methodologies, relates back to the idea or goal of striving for empirical generalization, but according to van Manen (2016a), empirical generalization is impossible within phenomenological methodologies. As such, when considering the term *sample* from a phenomenological perspective, the goal of sample selection referred to a population that can provide a representative example of the lived experience being investigated. Purposive, or purposeful, sampling, was used to select three participants from the study population to participate in this phenomenological research effort, and snowball sampling was be used to find additional participants as needed until saturation had been attained.

Data saturation. In phenomenological research, data saturation plays an influential role in the determination of the sample size. Like other qualitative research studies, in phenomenology, data collection continues until data saturation is reached (Creswell & Poth, 2018; Stake, 2010). Still, the meaning of the term *data saturation* differs between phenomenological research and other qualitative inquiries, which can have implications for the sample size needed to ensure saturation has been reached (Krathwohl, 2009; Creswell & Poth, 2018; van Manen, 2016a). Most commonly seen in qualitative inquiries, data saturation is attained when no new information is being gathered from study participants during the data collection process (Krathwohl, 2009; Creswell & Poth, 2018; van Manen, 2016a). At times, attaining saturation involved collecting data from 20-30 participants (Creswell, 2014). Yet, van Manen (2016a), a seminal researcher in the area of phenomenology, argues that saturation in phenomenological studies differs from saturation in other qualitative studies because it is attained when enough information and context has been collected to write a rich description about what the essence of the phenomenon is like for those persons who have lived the phenomenon.

Data saturation and study design. Even though Creswell (2014) mentioned the typical sample size for a qualitative study ranges from 20–30 participants, in the following excerpt, Creswell (2014) also supported the notion that the design of the study influences the sample size, while also providing additional insights about the most commonly used sample size ranges for the different types of qualitative studies:

> I have taken the position that sample size depends on the qualitative design being used…. From my review of the many qualitative research studies I have found narrative research to include one or two individuals; phenomenology to typically range from three to ten; grounded theory, twenty to thirty; ethnography to examine one single culture-sharing group with numerous artifacts, interviews and observations; and case studies to include about four to five cases. (p. 189)

Sample size. Moustakas (1994) explained that, for phenomenology, the criteria for locating and selecting participants in the study is not typically determined in advance. Instead, the researcher is expected to determine, "How many examples of concrete experiential descriptions would be appropriate for this study in order to explore the phenomenological meanings of this or that phenomenon" (van Manen, 2016a, p. 353). In fact, to accomplish the goal of attaining data saturation in phenomenological research, investigators have performed studies with single participants (Padilla, 2003) and upwards of 300 participants (Polkinghorne, 1989). In 1984, Dukes offered a recommendation of studying three to ten participants, a recommendation supported by Creswell (2014) in the excerpt above. This was also the recommendation that was adhered to for the current study.

Data Collection.

The goal of the phenomenological data collection process is to capture the common, lived experiences of study participants and to organize the collected data in such a way it will be ready for data analysis (van Manen, 2016a). This section offers a detailed discussion of the phenomenological data collection instruments, techniques, and organization practices used throughout this study. The tools and techniques were chosen with the support of the literature to ensure the overall aim of the study was met and questions asked by the study were answered.

Instruments. In phenomenological research, the researcher plays a central role as an active participant in the data collection process of a study (Stake, 2010; Lincoln & Denzin, 1998; Moustakas, 1994). The two primary data collection activities the researcher utilized for the current study included journaling and interviews. Interviews were captured using audio-recording, and contextual details that occurred during the interview process were documented via note taking to ensure important non-verbal or behavioral cues were available for reference during the data analysis and reporting process.

Journal. At the beginning of the data collection process, the researcher maintained a journal to collect data about personal assumptions and biases. An important part of the transcendental, phenomenological inquiry requires the researcher to "set aside prejudgments regarding the phenomenon being investigated" (Moustakas, 1994, p. 22). The process of setting aside personal experiences to allow the investigator to gain a fresh perspective is the epoche process, sometimes called bracketing (Creswell & Poth, 2018). Moustakas (1994) further explained the purpose of the epoche to the transcendental, phenomenological study process:

> In order to launch the study as far as possible free of preconceptions, beliefs, and knowledge of the phenomenon from prior experience and professional studies – to be

> completely open, receptive, and naïve in listening to and hearing research participants describe their experience of the phenomenon being investigated. (p. 22)

Interviews and audio-recordings. Once the researcher extracted personal experiences, assumptions, and biases, the data collection process required the researcher to manage all activities related to conducting and managing the interview process. The interview process depended on the accurate capture and reporting of participant responses using audio-recording and word-for-word transcription. The long, or in-depth, interview is the typical method used by researchers to collect data on the topic and research questions (Moustakas, 1994; Creswell & Poth, 2018), as such it was also be employed for the current study. A phenomenological interview is usually informal, therefore the researcher used open-ended comments and questions to interact and evoke a comprehensive account of a participant's experience with the phenomenon (Moustakas, 1994).

Interview guide. The eventual goal of the interview process was to generate a textual and structural description of the experience that shares an understanding of the mutual experiences of those who participated in the interview process (Creswell & Poth, 2018). Appendix A contains the initial script to be used during the interviews with IS professionals. The researcher designed a broad first question to evoke a rich description of the participant's experience of the phenomenon, as encouraged by Moustakas (1994). Each question in the interview guide related back to the research questions to ensure the overall problem of the study was addressed. Still, it should be noted that the script used during the interview process may have been modified during the interview, depending on the responses elicited from study participants, as it was necessary for the researcher to ask follow-up questions to extract additional details or clarification from the study participant so the goal of generating a richer description and understanding could be met.

According to Moustakas (1994, p. 114), this is typical of transcendental phenomenological research, because "although the researcher may in advance develop a series of questions aimed at evoking a comprehensive account of the person's experience of the phenomenon, these are varied, altered, or not used at all," as the participant discloses their experiences during the interview process.

Note-taking. The data collection process for this study also involved note taking during the various interactions to ensure relevant contextual activities were not overlooked during the various interactions between the researcher and participant. Indeed, it is imperative to capture and report on relevant contextual cues, such as behaviors, impressions and nonverbal signaling (Sutton & Austin, 2015), therefore the researcher's role also included taking field notes and keeping track of elements that could not easily be captured in recordings. Notes taken by the researcher during the interview process were incorporated into the transcript to ensure the context cues are recorded and maintained for analysis.

Data collection techniques. The transcendental, phenomenological approach followed specific and systematic steps to ensure the final report focused on the phenomenon under investigation from the perspective of participants rather than the interpretation of the researcher (Moustakas, 1994). According to Creswell and Poth (2018), these two main data collection steps within the phenomenological procedures include bracketing out the researcher's own experience with the identified phenomenon and collecting data from persons who have experienced the phenomenon with in-depth interviews. This section describes how these data collection techniques were accomplished in the current study.

Journaling personal experiences. Bracketing out personal thoughts and experiences enabled the researchers to set aside the biases and assumptions about the phenomenon of IS

professionals working to prevent social engineering vulnerabilities in U.S. businesses (Moustakas, 1994). Journal entries became the basis for developing the epoche. The researcher purposefully reflected upon each of the research questions and wrote journal entries to capture her personal thoughts and experiences related to the questions being asked in the study. Findings from the epoche process were bracketed out prior to interviewing study participants, so the researcher could remain open to hearing the descriptions of the phenomenon of study participants, as described by Moustakas (1994). Once collected, the researcher compiled and analyzed the reflections written in the journal to identify what underlying assumptions and biases existed that had the potential to affect the data collection, analysis, and reporting.

Inviting candidates to join the study. Prior to the interview, a series of questions were developed to elicit experiences related to the phenomenon and the aim of the study. The questions were used as a guide throughout the interview process, but as the interaction and exchange between the interviewer and participant ensued, questions evolved or were omitted as the participant shared their experiences. Once the initial questions were developed, the researcher initiated contact and invited candidates to join the study. If candidates declined to participate, the researcher asked candidates to refer other persons working in the same industry and region that the researcher could invite to participate in the study. Throughout the study, candidates, and subsequently participants, were assured that any identifying information about the participant and their employing organization would not be disclosed. To ensure confidentiality was maintained, identifying information was extricated from the transcript and final report, and was replaced with unidentifiable pseudonyms or non-identifying terminology.

Interviewing participants. Once a candidate agreed to participate in the study, the researcher asked participants to join in the research process to help determine the most

appropriate method (e.g., face-to-face, phone, web conferencing tools, etc.) and location to conduct the interview to ensure participants were comfortable enough to speak their truth, while also ensuring the aim of the study is met. Once the details surrounding the interview were worked out, the researcher scheduled the interview. During the interview, audio-recording was used to capture responses from the participant. Once the interview was complete, the researcher transcribed the recording into a Microsoft Word document. After the interviews were transcribed, participants were asked to review and check the transcript for accuracy purposes.

Data organization techniques. The techniques employed throughout the data organization process were essential for ensuring valuable data and insights are not lost due to reliance on the researcher's memory and recollection of the experience (Krathwohl, 2009). Once the interviews were completed, the researcher used a password-protected jump drive to house all documents and files relevant to the study. All files and documents relevant to the study were maintained and secured on this password-protected jump drive and stored in a safe location only accessible by the researcher.

Documents to be secured. The researcher maintained Microsoft Word documents and containing raw data, such as transcribed interviews, journal entries, and notes capturing contextual cues. Analyzed data, where the transcriptions were collected, coded, and clustered into themes, were also saved and stored in Microsoft Word documents and Microsoft Excel workbooks. Additionally, a Microsoft Excel worksheet was maintained to keep track of any items destroyed for the purposes of protecting participant anonymity.

Audio-recordings. Once the interview was complete, the researcher kept the recording device and audio-recording on her person until she returned to a secure office that requires a key to a deadbolt to obtain entry. Audio-recordings were transcribed by the researcher into a

Microsoft Word document and saved to the designated secure file location. Copies of original audio-recordings were maintained on the password-protected jump drive and stored in a safe location only accessible by the researcher. Audio-recordings will be maintained for the period required by the Institutional Review Board at Liberty University.

Journals and notes. The researcher utilized a journal to reflect on and bracket out thoughts and assumptions about her experiences with the investigated phenomenon. Journal entries and other contextual cues captured in the note-taking process were input into Microsoft Word documents. These documents were maintained with transcription files and coded documents on the password-protected jump drive.

Data security. The researcher followed protocols established by the IRB at Liberty University related to record retention and data destruction. Research data and records will be stored securely on a password-protected zip drive for three years following the study, and credentials of the researcher will be required to access or retrieve the files. When the zip drive is not in use, the drive will be stored in a safe that can only be accessed by the researcher. After three years, all electronic records will be deleted.

Once interviews were completed, the researcher kept the recording device and audio-recording on her person until she returned to a secure office that requires a key to a deadbolt to obtain entry. Audio-recordings were transcribed into a Microsoft Word document and saved to the password protected zip drive, and all identifying information was removed from transcribed files to protect the confidentiality of the participants. Raw data from the audio-recordings were saved to the password-protected zip drive following the transcription process, and the original recordings were erased from the recording device. After three years, all audio-recordings will be destroyed. Any hard copies of notes were shredded and recycled once electronic copies were

created and saved to the secure file location. Any other exchanges between participants that leave a documentation trail, such as email messages, require secure credentials to access and will not be disclosed or shared with anyone outside the study.

Summary of data collection. A transcendental phenomenological research effort follows systematic steps to ensure the collected data meets the goals of the study (Creswell & Poth, 2018). Two specific data collection activities the researcher engaged in included bracketing out their own experiences with the phenomenon and collecting data from people who have experienced the phenomenon (Moustakas, 1994; Creswell & Poth, 2018). The researcher accomplished the first task utilizing journal entries to document her personal experiences with the phenomenon of IS professionals defending U.S. businesses against social engineering attacks. Then, the researcher solicited participants to interview who have experienced the phenomenon. Interviews were scheduled, audio-recorded, and transcribed by the researcher, and the participants were involved in the process by reviewing and checking the transcription. The researcher also took notes during the various interactions with participants to log important non-verbal or behavioral cues, which were referenced during the data analysis and reporting process. Participant information remained confidential and secure to ensure the study created minimal risk to the participant. Files related to the data collection and analysis process were maintained and secured on a password-protected jump drive and stored in a safe location only accessible by the researcher. Protocols established by the IRB related to record retention and data destruction were followed to ensure the protection of study participants.

Data Analysis

According to Stake (2010), the data analysis process of a research study deals with taking things apart followed by searching for elements and associations between elements. After taking

everything apart, the researcher uses their critical thinking and analysis skills, as well as their previous experiences, to pull everything back together (Stake, 2010). Consequently, the quality of the data analysis is dependent on the ability of the researcher to collect data, sort and classify the data, and interpret these clusters of data in such a way that extracts meaning (Stake, 2010).

Coding process. The current study utilized coding to sort all the collected data by themes and their relevance to the study. The researcher handled the coding and analysis process manually. Microsoft Word and Microsoft Excel were used to support the activities related to coding the collected data. The study followed a systematic data analysis process typically used for transcendental, phenomenological studies, as outlined by Moustakas (1994) and Creswell and Poth (2018). According to Moustakas (1994), the data analysis process begins when the transcribed interviews are in front of the researcher. It is at this point the phenomenal analysis of the transcriptions begins. During the phenomenal analysis procedure, the researcher will organize the data using a process called horizontalization, whereby every significant statement that is considered relevant to the research effort will be listed and given equal weight (Moustakas, 1994). These statements are important for providing the understanding about how the subjects experienced the phenomenon (Creswell & Poth, 2018).

The next step in organizing the data involved clustering statements into themes, or clusters of meaning (Moustakas, 1994; Creswell & Poth, 2018). For this research effort, statements were initially clustered together by the research question being addressed. From this point, the synthesis and construction process began, as the researcher used the clusters of meaning and themes to write about the description of the experience. According to Moustakas (1994), "From the textural description, structural descriptions, and an integration of textures and structures into the meanings and essences of the phenomenon are constructed" (pp. 118-119).

Summary of data analysis. In sum, the data analysis involved the researcher manually breaking apart the data that had been collected using sorting and coding techniques, as described by Moustakas (1994) and Creswell and Poth (2018). The software tools that were used to support the sorting and coding activities included Microsoft Word and Microsoft Excel. Once coded, the researcher clustered statements together by the research question being addressed. The researcher then pulled each of these parts back together to synthesize the meaning and essence of the phenomenon into a rich, textural description in the final report. The richly descriptive final report accomplished the purpose of the study by providing insight into how IS professionals make sense of their lives and experiences as they address and prevent vulnerabilities to social engineering attacks.

Reliability and Validity

The validation process in qualitative research studies, according to Creswell and Poth (2018), endeavors to measure the accuracy of the results from the viewpoints of the researcher, study participants, and readers. Looking at the topic through these various lenses contributed to the validation of the study effort. Qualitative research offers various strategies to ensure the study is reliable and valid, and the use of multiple validation strategies is recommended to build credibility for study findings (Creswell & Poth, 2018). This section explains the role of reliability and validity to generate understanding from these various lenses in the current phenomenological research study.

Reliability. In qualitative research, *reliability* is synonymous with the term *consistency (*Krathwohl, 2009). For a qualitative study to be deemed reliable, it is important to seek consistency in the methods used for collecting and analyzing the data. Krathwohl (2009) explained that the nature of the study determines where readers will seek out consistent practices.

In qualitative research, establishing a clear audit trail of the research process, including crucial aspects such as making transparent decision about the method selection, data collection tools and procedures, and data analysis process, can provide readers with everything they might need to decide about the consistency of research findings (Slevin & Sines, 1999). According to Creswell and Poth (2018), reliability can also be improved in qualitative studies "if the researcher obtains detailed field notes by employing good-quality recording devices and by transcribing the digital files" (p. 264). This is echoed by Slevin and Sines (1999) who explained that the use of audio-recording devices and "subsequent verbatim typing of interviews into transcripts in the study assured consistent and accurate recording of data" (p. 86). Additionally, presenting a participant's unaltered response to an interview question in the final report demonstrates a truthful, consistent account of the data to readers (Slevin & Sines, 1999).

Creswell and Poth (2018) implied that too many coding staff and analysts can complicate the analysis process of a research effort. To address this potential shortcoming in the current study, the number of persons engaged in the data collection, coding, and analysis activities were limited to a single researcher, rather than splitting project responsibilities among multiple coders and analysts. The same researcher who interviewed and audio-recorded the participants was also responsible for taking detailed notes to capture contextual, nonverbal cues and for transcribing and coding the interviews. By limiting the number of researchers to a single person, the researcher ensured greater consistency in the assignment of themes and codes (Krathwohl, 2009).

Validity. Validity in a qualitative research effort centers on how well the findings embody reality (Slevin & Sines, 1999). According to van Manen (2016a), the nature of the study plays an important role in how the validity of a study should be measured. Indeed, van Manen (2016a) argued, "a common problem for phenomenological researchers is to be challenged in

defending their research in terms of references that do not belong to the methodology of phenomenology" (p. 347). van Manen further purported that mixing methods from one type of study to another can instead cause misinterpretations if researchers do not recognize that concepts should adjust and change when the nature of the study changes. Accordingly, the chosen validation and reliability strategies to be employed for the current study were selected with the nature of the study, a transcendental phenomenological qualitative research study, in mind.

Triangulation. According to Stake (2010), the process of triangulation involves purposefully, habitually reviewing and considering the gathered evidence from various points of views utilizing a range of techniques. It is the triangulation process that establishes that the study is credible (Creswell & Poth, 2018). In the current study, both the researcher's point of view and the point of view of participants were captured during the data collection process. The self-reflection process engaged in by the researcher allowed evidence to be collected about the researcher's point of view into journal entries that were conveyed to readers in the epoche. Documenting the researcher's personal experiences, beliefs, and biases in this manner may provide insights and generate greater understanding to readers about how the data were interpreted. The study also gathered triangulated evidence from study participants through the interview process. Because study participants came from different IS functions and were employed across three distinct industries—some known for their more stringent regulations than others—the process of triangulation occurred organically as the researcher accepted responses to the interview questions and sought insights into common experiences. Not only were journal entries and interview transcripts analyzed, but also triangulation occurred during the comparison of themes. Last, after interviews were transcribed, participants were asked to review and check

the transcript for accuracy purposes. Member-checking is another activity that can reinforce the validity of a phenomenological study, as participants can clarify whether the researcher accurately captured the essence of the experience (Moustakas, 1994).

Saturation. Research suggests that a phenomenologist knows data saturation has been reached when no new information is being shared (Krathwohl, 2009; Creswell & Poth, 2018; van Manen, 2016a). Still, according to van Manen (2016a), collecting data for a phenomenological research differs from other studies in that an investigator "looks not for sameness or repetitive patterns. Rather, phenomenology aims at what is singular and a singular theme or notion may only be seen once in experiential data" (p. 353). Instead, data saturation in phenomenology occurs once enough "experientially rich accounts" (van Manen, 2016a, p. 353) have been collected such that the researcher can accurately capture and convey the lived experience to readers in a rich textural description. Accordingly, the researcher recognized that data saturation had been reached when adequate information and context has been collected to write a detailed account about what the essence of the phenomenon is like for those persons who have lived the phenomenon. The rich description is included in Section 3 of the final report.

Transferability. The rich description of the phenomenon was also be considered final strategy employed by the current study to address the final leg of triangulation--the point of view of readers. It is the rich, thick description that allows readers to decide whether the findings are transferable between the researcher and study participants (Creswell & Poth, 2018). The rich, thick description allows anyone reading the study to decide whether the characteristics of the setting and circumstances could happen elsewhere, which in turn allows readers to envision whether the findings might also be assigned to other settings and circumstances. To accomplish this strategy in the current study, the researcher not only transcribed the raw data soon after it

was captured, but the researcher also revised the transcription to include additional, contextual descriptions captured in the notes that aided in the analysis and coding process, to ensure the details and interconnected pieces of the experience lived by participants were adequately described to readers.

Summary of reliability and validity. Following the examples provided in the qualitative and phenomenological literature, various strategies were employed to ensure the study was both reliable and valid. Reliability was addressed through the establishment of a transparent audit trail of the research process and by following interview best practices. These best practices included using audio-recording devices during the interview process and immediately transcribing the interview word-for-word, while also adding contextual cues captured from the detailed field notes. To further enhance consistency and reduce complications that occur in the coding and analysis process, only one researcher was responsible for all processes related to the data collection, coding, and analysis activities throughout the study.

With the goal of making sure findings accurately represent reality (Slevin & Sines, 1999), validity was addressed by the utilization of triangulation strategies throughout the research process. Journaling was used to bracket out experiences, beliefs, and biases to capture the point of view of the researcher. Interviews and note-taking were used to collect data from the point of view of the study participant. A rich, textual description was written and included in the final report, conveying a truthful account of the phenomenon to readers who will decide whether findings can be transferred to other situations, thus engaging the reader's point of view. Because data saturation for phenomenological studies tends to be based off having enough "experientially rich accounts" (van Manen, 2016a, p. 353) to accurately convey the essence of the phenomenon to readers, the researcher acknowledged that data saturation had been reached when enough data

had been gathered to write a rich, thick description that allowed readers to envision and understand the situation.

Transition and Summary of Section 2

This section concludes Section 2, the Project, which establishes how the investigation into the phenomenon of IS professionals protecting U.S. businesses from social engineering attacks was conducted. The section began with a reexamination of the purpose of the study and background of the problem and transitioned into the role of the researcher, who played an essential part not only in designing the study, but also in protecting the study and participants, collecting, maintaining, and securing the data, and analyzing, interpreting, and reporting the findings of the study. Once the role of the researcher was described, attention shifted to the participants of the study. As it is important for the population to represent the group being studied in phenomenological studies (Krathwohl, 2009), to join the study the participant must have been both willing and qualified as an IS professional working in healthcare, financial services, or education fields who held experiences with protecting their company from social engineering within the past year. The researcher used purposive and snowball sampling to identify candidates for the study, and once candidates agreed to participate, the data collection process commenced.

The data collection process for this study primarily consisted of journaling and interviews, which was supplemented by note-taking to capture nonverbal signaling or context cues that could not be captured by an audio-recording. An interview guide was used to facilitate the interaction between the researcher and participant during the interview process, and audio-recording was used to capture and record the interview. Both journaling and interviews were used to capture the different the points of view of the researcher and the study participants,

which was important to assure readers of validity and triangulation in the qualitative research process. Once an interview was conducted, the audio-recording was transcribed into a Word document. All data records were saved on a password-protected jump drive that will be stored in a secure location for three years following the close of the study.

The study followed the systematic data analysis process typically used for transcendental, phenomenological studies, which typically starts when the transcribed interview is in front of the researcher (Moustakas, 1994; Creswell & Poth, 2018). The findings from the data collection process were analyzed, coded, and used to write a rich, textual description for the final report. The rich description allows readers to decide if findings might be assigned, or transferred, to other settings and circumstances, which accomplished the third and final aim of the triangulation process—to address the point of view of readers. The strategies employed throughout the study attempted to assure reliability, consistency, validity, triangulation, saturation, and transferability so that the findings shared in the final report can be trusted as an accurate representation of the reality experienced by IS professionals as they protect their organization from social engineering attacks. The study now transitions into Section 3, Application to Profession Practice and Implications for Change. Section 3 closes out the research effort with a presentation and discussion of the findings, applications to professional practice, recommendations for action, further study, reflections, and final conclusions.

Section 3: Application to Professional Practice and Implications for Change

Section 3 begins with a brief overview of the study. This overview revisits why the study is important and provides a summary about how the study was accomplished. Next, the findings of the study are presented along with an analysis and implications of the findings. Then, relevant applications to professional practice, recommendations for action, and suggestions for further study are outlined. The study closes with reflections of the researcher, a summary of the study and findings, and conclusions.

Overview of the Study

This transcendental phenomenological qualitative study was conducted to examine how IS professionals working in U.S. businesses make sense of their lives and experiences as they address and prevent vulnerabilities to social engineering attacks. The phenomenological process outlined by Creswell and Poth (2018) guided the effort, enabling the researcher to formulate the description of the investigated phenomenon. The primary objectives of the research effort were to give IS professionals an opportunity to voice their personal lived experiences related to the phenomenon, to describe these lived experiences, and to develop an understanding of the phenomenon by interpreting and translating their responses into themes and codes that could be used to capture the overall essence of the shared experience.

This study presents the major findings of this phenomenological qualitative inquiry into the lived experience of six IS professionals defending their organization against social engineering attacks. Ten common themes were identified across participants, which, when combined, capture the overall essence of the experience of the phenomenon. While several of the findings were consistent with previous literature on the topic (Lineberry, 2007; Ekwall & Rolandsson, 2013, Zhan et al., 2015; Orgill et al., 2004), a few findings were not previously

identified in the body of literature. The overview opens with the researcher's epoche and concludes with demographic information of participants and a brief description of each study participant. These pieces are provided to help readers (a) better understand the researcher's background and potential biases and (b) more readily envision the responses presented in the findings.

Epoche. Just a few months ago, I received a phone call from someone who wanted to conduct a survey about our organization's cybersecurity measures, and they were offering $100 for me to participate. First, they would ask me some screening questions to see if I were eligible to participate based on my knowledge of our systems. Prior to my investigation into the topic of social engineering for my dissertation topic, I probably would have tried to help my fellow researcher—whom I had not confirmed their credentials—achieve their research goals. Instead, as their questions became progressively more direct about our information systems and security systems, I responded with, "I prefer not to answer." This could have been a legitimate survey. But the reality is, $100 is not worth the damage that can be done at my workplace, to my students, and to my colleagues if it was a social engineer gathering reconnaissance about my employer. When the phone call ended, I felt as if I had been extremely rude to the caller. I did not know, and still do not know whether it was a researcher or someone with harmful intentions. While I felt paranoid, I also wondered if I had overdone it. On the other hand, I felt somewhat empowered by my ability to say "No, I'm not going to give you answers that could put us in harm's way."

Surprising perspective. Because of my uncertainty, I went to visit a colleague who is considered our resident cybersecurity expert. I quickly discovered he had received a similar call the day before and had agreed to participate in the survey. He informed me,

> Hey, if it is a social engineer, they're going to get the information from someone on this campus. I consider it IT's job to have a strong enough defense in place. If they are preparing to perpetrate an attack, it doesn't matter what information I give them, they better be prepared for it.

His response surprised me, because research and cybersecurity reports repeatedly state the importance of educating employees and creating a security culture to build a strong defense. After reading these reports, I had convinced myself that I, as an employee, am both responsible and accountable.

Nonetheless, after hearing this divergent point of view, I realized that not everyone accepts defense against social engineering attacks as part of their responsibility. And, as seen by my colleague, some may simply refuse to accept responsibility for defending the organization against cyberattacks as part of their job role and function. This interaction led me to question how an IS professional might deal with the wide spectrum of beliefs about security roles and responsibilities across their organization. I mean, here was a *cybersecurity* expert who believes education will never be enough, and everyday employees won't be the ones held responsible when an attack is successful—the IT team will be accountable. So, how do IS professionals deal with an employee like this one, who considers his/her role as important to pointing out potential holes/vulnerabilities in the current system? Do they ignore them? Shut them down? Punish them? Educate them more? Or do they find ways to use them to their advantage? Currently, many cybersecurity reports focus on what needs to be done, what is being done, what is done well or poorly, a lot or very rarely. Have we looked at the people involved, their attitudes and beliefs? Have we considered how these attitudes and beliefs influence their decisions and actions related to creating a strong defense against social engineering attacks? A look into the

research tells us very little about these attitudes and beliefs, much less how these attitudes are influencing people.

Background of the researcher. I began working as an IS professional at a startup in 2005 after earning my BBA in CIS. While I was aware of the need to keep customer data confidential, from the perspective of a newbie in the business, I was mostly aware of the importance of not sharing one customer's data with anyone besides the customer and my colleagues. Fast forward six years, and I found myself working in the Office of Institutional Research for a regional, four-year public university. My job at the time included managing and reporting on student information to various internal and external entities. The expectations regarding the sharing of student information were much more clearly defined under FERPA than I had experienced in my earlier years.

Still, I would not say I was ever on the lookout for a social engineering attack, and if I had received a phishing email during that time, I was unaware of it. Most data requests were reports we did on a regular basis or had been vetted by the director before being assigned to me. We had a system in place for requests that fell outside the scope of our ongoing reporting needs, which included following a specific protocol to vet whether the request could be sent to the requestor. Beyond initial training and signing the confidentiality agreement, I do not recall ever receiving formal training about the dangers of social engineering attacks or the need to be aware about the cybersecurity threats. Now, I am a faculty member responsible for teaching, advising, research, and service. I am still responsible for keeping student information private and confidential. In my time in this capacity, it has only been in the past year that I recollect having seen one email from the IT team about cybersecurity threats to universities—and this email came

after a successful attack had already been perpetrated across the entire campus—affecting students, faculty, and staff alike.

So truly, it has only been in the past year, while working on my dissertation topic, that I have become significantly more aware and enlightened about the dangers of social engineering in the workplace, not only for people working as IS professionals, but also for people in all areas of business. As far as my personal experiences with preventing social engineering vulnerabilities go, I have always strived to follow protocols regarding maintaining customer confidentiality and data. Integrity and work ethic are key characteristics for data workers. Yet, as I've learned in my research learning all the ins-and-outs of social engineering, that might not be enough to protect a person or their organization from their own human frailties. So, while I've never been contacted by our IT department to learn my credentials have been compromised or have resulted in a breach, that doesn't mean that I have not inadvertently contributed to the reconnaissance or advancement of a social engineering exploit--which is scary and confounding all at the same time. Indeed, attacks are so sophisticated now, that a person can help a social engineer and never know they were a pawn in an attack. So, while I do my very best to follow protocols, I have no idea if I've been the victim of a social engineering exploit.

Even so, if I'm being completely honest with myself, I probably have. I know I've been targeted—be it part of a mass phishing scheme at my workplace or via social media. And all it takes is one wayward click. One moment of curiosity where I let my guard down and clicked the wrong link or responded to an email I shouldn't have. Social engineers thrive off natural human tendencies of laziness, fear, trust, curiosity, and more, so, again, there is a strong possibility that I have contributed to some form of social engineering attack without even knowing it. Still, I do not *feel* like a victim, and while I do have various biases about the topic, the goal of this research

effort is not to make a point from my own personal experiences and biases. I am doing this research to better understand what my sisters and brothers in IS fields are experiencing, in hopes that perhaps we can gain some insight about whether we need to do things better and make things better for current and future employees in the field.

Demographic information. This study included six IS professionals working in U.S. businesses across central and northwest regions of Louisiana. Five participants were acquired from a list of professional contacts who responded to the recruitment email. The final participant was attained through the snowball sampling process. All participants (n = 6) reside and practice in the state of Louisiana and identified themselves as being 18 years of age or older. All participants (n = 6) identified themselves as having worked for their current employer for at least one year, and all six acknowledged that their employer experienced social engineering threats or attacks within the previous year. Two participants were represented from each of the industries included in this study, health care, financial services, and higher education. Half of the participants (n = 3) were male and half were female (n = 3). All indicated having earned a bachelor's degree or higher, but only half (n = 3) attained their degree in a computer-related field. Most participants (n = 4) worked in security-related positions, while the remaining two participants did not consider their primary job function to be security-related. All six participants were full time employees.

Participant characteristics. The researcher chose to present each participant with the following non-identifiable pseudonyms: Participant 1 (P1), Participant 2 (P2), Participant 3 (P3), Participant 4 (P4), Participant 5 (P5), and Participant 6 (P6). Each participant is presented using the selected pseudonym throughout the study, including all transcriptions and interactions. This ensures confidentiality is maintained throughout the entirety of the research process. The

characteristics of each participant were gained from the audio-recordings and interview transcriptions, which contained their thoughts and reflections on their experiences about the current phenomenon. While the experiences of each participant varied by their primary role, all participants were open to and engaged with the interview process and eager to provide insights into their experience of defending their organization from social engineering attacks. Accordingly, the exchange during the interview process between the researcher and participants were both productive and focused towards achieving the objectives of the study.

Participant 1 (P1). P1 is a male IS professional with approximately five years' experience in the field. He has been working in a security capacity for the last six months. P1 joined a startup in the healthcare field after working in the retail sector where his primary experiences dealt with hardware and "geeking out on toys." When he was approached to join the fledgling organization, the company was comprised of less than 10 people, and they needed someone who could dabble in a little bit of everything IS-related. While P1 earned a bachelor's degree, it was not from a computer-related field, so he knew he would be in for new challenges and experiences when he joined the team.

Since his coming on board, the organization ballooned to nearly 60 employees. The responsibilities of his position grew as rapidly as the company did, including his being assigned the HIPAA compliance officer for the organization. This assignment is the reason he first began dabbling in a more security-centric capacity. Yet, even though he added two additional IS professionals to the team, P1 remained the sole security personnel. He works full-time and, until recently, worked a substantial number of overtime hours, explaining that security was a 24/7 job, and

> If they [employees] don't stop working, then you don't stop working. So, if they don't learn work-life bounds, then you can't have any as a security professional. Cause if the vice president's 24/7, then his account's 24/7. If his account's 24/7, then phishing attempts are 24/7.

Still, even though P1 described the fast pace and grueling hours as "rough" in his first years with the company, he also believes "it's getting better." P1 clearly identified his lived experiences and the essence of those experiences defending his organization against social engineering attacks.

Participant 2 (P2). P2 is a director of information systems at a startup in Louisiana that operates primarily in the healthcare sector, although the services offered by the organization also spans into the financial services industry as well. P2 earned her Bachelor's in Computer Information Systems degree from a local university and was actively recruited to join the rapidly growing company upon her graduation, where she found her skills in systems administration to be indispensable to her success. She was one of the first employees of the company, and she is fully "invested in our company, and the well-being of our company, and the well-being of our employees."

P2 is one of the three female participants in the study and one of only two participants not working in a security-related role. Still, because she is one of the founding members of the company, she believes that her biggest contribution to defending the organization against social engineering attacks is her role in establishing culture that prevents the negative consequences from happening "to my employees *or* to the company as a whole." P1 regularly trains others at her company to be more aware of social engineering attacks, but she also feels responsible for "helping everybody else in the company and helping report these things to IT" when they

happen. She also openly admitted her role in encouraging another colleague to inadvertently succumb to an attack, which allowed her to discuss why she continuously advocates for communication, training, and "learning from your experiences" when it comes to dealing with the phenomenon.

Participant 3 (P3). P3 is the second participant not working in a security-related role, instead, she is primarily responsible for responding to data requests for her university. She earned her bachelor's degree in a computer-related field decades ago, and she has extensive experience as an IS professional in her area of expertise. While she is presently a full-time employee and director of her department, she is also currently enrolled in a program to earn a master's degree in a computer-related field. While P3 did not have the most experience with dealing with social engineering attacks of the other participants, claiming, "there's not been a lot of incidents that have happened" in her area, her willingness to communicate openly about her experiences helped the researcher both confirm the overall essence and discern additional themes that might have been overlooked without her unique perspective.

P3 was the first participant to mention that her university did not have someone designated as the security point-person, which she felt was key to moving the idea of a security culture from a "concept" to "something people can get behind." She also called herself a "mama bear" when describing how protective she felt about the data, her customers, and the university she serves stating, "I consider it meaningful to the extent that I have saved somebody else from having to deal with that. I'm one of the gatekeepers." And even though P3 believed others at her university "would probably want to kill me for saying this," she also felt very strongly about following and updating policies and procedures to keep the organization safe because, "Policies and procedures, I think, give you a framework to be able to respond consistently."

Participant 4 (P4). P4 is the second male IS professional to participate in the study. He is the first participant to offer insights from the C-level, as he is the CIO of his institution. Of all participants, P4 held the most extensive IS experience related to the phenomenon under investigation. He also held the greatest amount of experience, over 18 years, working in various roles in his chosen industry, banking. His previous positions ranged from being "teller," followed by taking on a "network security administrator" role. He spent time as the "information security officer and systems officer," before moving "to the risk department" where his role shifted to "audit and information security." His unique background gave him a plethora of knowledge and experiences to pull from throughout the interview process.

P4 good-humoredly confessed to being "OCD and paranoid about everything" in terms of securing his financial institution from security-related problems, but he was not joking around when he shared how he felt when a social engineering vulnerability was exploited in his industry, declaring, "Scary! It's *scary*! Cause you think, [if] this could happen to them…." Following the interviews, it became apparent that, of all the organizations and industries represented in the current study, P4's company was in the best position to anticipate and circumvent social engineering attacks. Whereas the others were primarily in the position to react and remediate. In fact, when asked if he could share one of the times he had to deal with a social engineering at his workplace, he could not name a specific incident like those from other industries. Instead, he explained they have been able to avoid them because, "we have layered security" which included considerably more training and testing protocols than mentioned by any other participant. Whether driven by industry expectations, motivated by P4's fear of the potential consequences, or compelled by his experience, P4 and his team appeared to be doing many things right in terms of defending their organization against social engineering attacks.

Participant 5 (P5). P5 is the final female participant in the study and the second participant to have a bachelor's degree in a non-computer-related field. P5 is the only participant who joined via the snowball process when P4 invited her to tag-team with him during his interview due to her role as the Information Security and Cybersecurity Officer at their bank. Where P4 had been at the company for three years, P5 was in her sixth year. She previously worked in commercial lending before shifting to her information security position two years prior. It was clear that P4 and P5 worked very closely alongside one another to keep their company running smoothly. P5 explained the differences between their roles at the company.

> On my side, as information security officer—I'm more with like, the vendor due diligence, the training of employees. You know, the checks and balances of who's all doing what. Different logs and stuff like that. He's more the…you know, cause he's information officer. He's more the technical [side of things] …. So, I'm the one that goes behind and says, 'Okay, well what are y'all doing. Make sure you're not doing things you aren't supposed to be doing…'

P5 revealed, "The first thing I did when I moved up here was start reading the FFIC books" to stay on top her new role and the massive number of regulations they are required to address. She, more than other participants, addressed the role of regulations and regulatory agencies in helping them be more successful than other industries in protecting their company from social engineering attacks. She shared, "I think banks are way heavier regulated then even health care, and definitely schools…. And [the audits are] *frequent.*" And while some might consider the regulations and regular audits a hassle, she felt that regulations were instrumental in ensuring they "take the measures to be secure." P4 agreed, claiming, "regulation protects the customer."

Participant 6 (P6). P6, the second participant from the higher education sector, is the also the second of two participants to join the study with a C-level perspective, as he is second in command of the IS function at his university. He is the third participant with a bachelor's degree from a non-computer-related field and the final male participant in the study. His role at the university includes oversight of the technology infrastructure across the entire enterprise and leveraging technology and people to achieve the objectives of the university. In terms of protecting the organization from social engineering attacks, his team primarily focuses on addressing issues through the implementation of control measures coupled with training and communication following an attack.

Not unlike the participants from the banking sector, P6 placed a lot of emphasis on the expectations surrounding institutions operating in the higher educational environment, arguing that culture of the industry is partially responsible for how his team responds to and implements countermeasures for social engineering attacks. Furthermore, reminiscent of P3, the other participant from higher education, P6 explained that the university he works for does not yet designate the responsibility of social engineering or cybersecurity to "a 100% defined security individual," explaining that while "it's something that we're talking about" everything always returns to the lack of available resources and funds, and "it always, unfortunately, winds up a major issue happening before the university says 'Okay we need to do something.'" Currently, addressing social engineering attacks falls to his staff of "two people who are system administrator, data center people" who deal with issues as they arise or are reported. Still, he recognizes "we need someone who is dedicated to those functions and roles that can monitor these systems and services and things and be proactive and not reactive when these kinds of things happen."

Presentation of the Findings

Research question 1. "What lived experiences do IS professionals have with preventing social engineering vulnerabilities in U.S. businesses?" From five verbatim transcripts, 129 significant statements were extracted in relation to addressing RQ1. Table 1 includes examples of significant statements with their derived meaning.

Table 1

Selected Examples of Significant Statements for RQ1

Significant Statement	Meaning
Once you've figured that out, then you've got to convince the whole culture of people who have been here for twenty, thirty years that they need to do things different.	Resistance to change is a very real issue for IS professionals.
So, are there tools to keep us from doing that? Yeah, maybe not. <<shakes head no>> I think it's more--I think awareness, and just…. Like, well, what [CIO] does. Sends out reminders, yeah. I would say, probably, the reminders are out maybe once a quarter. I'm just going on gut feel there.	Sending reminders is an important aspect of training and keeping it on the forefront of employee minds.
Training? I know we've gotten some after people have received links in their emails that were not legit, you know.	IS professionals use communication to stay ahead of social engineering attacks,
That's what I start to, "Okay, let me ask some people did you get it?" A couple of people come to me, "Hey, I got this weird text." And sure enough, um…	Training can help an employee make better decisions.
Making sure if someone shows up and says, "I'm so and so from CenturyLink" and you know nothing about it, that 1) you either call your manager or 2) you call this department—call somebody to say, you know, before letting them in, and don't let them in, you know, unless you get confirmation that "Yes, they're supposed to be there." We do reiterate that, a lot.	

Significant statements were then arranged into clusters, resulting in three themes. Table 2 contains examples of the theme clusters that emerged from their derived meanings.

Table 2

Theme Clusters with Related Derived Meaning for RQ1

Security cultivation	Train, test, repeat	Layers—not just for hair
IS professionals need other people and resources to build a security culture.	Preventing attacks is more difficult than reacting.	Layered security helps prevent social engineering attacks.
When people are involved, mistakes are going to happen.	Education and training is the heart of preventing SE attacks.	Training and controls go hand-in-hand.
With the right team and support, improving the security culture is possible.	Basic security knowledge is important for everyone.	Software tools and controls aid in the social engineering prevention process.
Someone needs to lead the culture change before other people will get on board.	Everybody, including board members, need security training.	It takes time, sometimes years, to build an effective security program--including all the layers.
Open communication helps when establishing a security culture.	Layered security controls help, but they have limitations.	Outsourcing security tasks helps IS professionals strengthen their defenses.
Resistance to change is a very real issue for IS professionals.	Social engineering training can be effective if it's repeated often.	While resources are important, they will always be limitations.

Theme 1: Security cultivation. Participants believed a culture of security must be cultivated to ensure social engineering attacks are prevented. To accomplish the development of a stronger security culture, participants discussed the importance of keeping lines of communication open, building key relationships, and designating responsibility to a single individual or team. P4 called communication among the various individuals and departments the "most important thing" and considered the lack of communication to be "the greatest risk that a business face." According to one participant, P2, sometimes fostering a culture that embraces open communication simple starts with her response to questions, "If I sent an email with an attachment and somebody calls in and says, 'Did you mean to send this? Did you actually send this?' I'm not gonna be annoyed with them for doing that." Thus, for an organization to adequately defend itself from social engineering attacks, the organization's culture must allow and encourage its people to ask questions without penalty or chastisement.

Subtheme 1: Find a partner, dosey doe. In addition to keeping lines of communication open, participants also noted the need to build strategic relationships as a necessary part of the work of changing the culture of an organization. P1 struggled with this culture shift firsthand as his startup began to mature, "culturally, right now, you're coming from a place where people didn't have any rules. And it was very much the Wild West." Still, he found ways to enlist the help of early adopters, which led those resisting the change to feel like they were falling behind, "So then they start using it, and then I don't have to do anything else. Because now [they] call me." People often resist changing the way things are done, and making the investment in strategic relationships is important to IS professionals hoping to enhance the security culture of their organization.

Subtheme 2: Tag! You're it. Prevalent across the statements of IS professionals in this study is the need for a designated person to be responsible for developing a security culture. A few study participants accepted this function as part of their primary role or assigned job function, but in other organizations, it was not always clear whether a position such as this exists, which may make it more difficult to get the people of the organization on board. When asked who was responsible for addressing the social engineering vulnerabilities at her workplace, P3 responded, "Somebody that we do not have working here at this university…. I mean, I think the culture is gonna come from... the people who take it up as a passion." Similarly, P6, the second participant from higher education said they also lacked a dedicated person to address security and social engineering issues. Still, he recognizes "We need someone who is dedicated to those functions and roles that can monitor these systems and services and things and be proactive and not reactive when these kinds of things happen." It is essential for an organization to designate someone with the responsibility of building and cultivating a stronger security culture.

Theme 2: Train, test, repeat. The predominant belief of every participant in this study is that the word *prevention* is synonymous with the words *training* and *education*. According to the study participants, to prevent social engineering attacks, the people of an organization must be aware not only of the danger, but also of their part in recognizing the threat and their expected response to the threat. IS professionals also acknowledge that exposure to security and social engineering will not be effective if training only happens once. For it to be effective, it must be iterated repeatedly. Three of the six participants shared the importance of making sure all employees received training upon hire and then annually thereafter. "It's once a year is the requirement. It is when you arrive, and then it's again the next year." In contrast, P4, a participant with access to greater training resources considered the onboarding and annual training a minimal requirement. Instead he tested his people more regularly using penetration tests, explaining, "I test every two weeks." In addition, IS professionals realize the importance of keeping social engineering attacks on the minds of their employees, as such, some use various reminders, such as banners across the top of incoming emails or emailing a quarterly newsletter to everyone in the company. Thus, to protect an organization from social engineering attacks, the people of the organization must be trained repeatedly to build awareness and withstand attacks.

Theme 3: Layers—not just for hair. IS professionals confessed that training works best to prevent social engineering attacks when used in conjunction with other electronic security controls. Participants also believed that layering security controls can play a significant role in reducing the overall impact of a social engineering attack. P5 discussed the role of these controls in protecting her organization, "We have the secondary controls in places so that, if they did [fall prey to an attack]… then we have these layers of security controls to catch it and completely

wipe it out before it does any harm." Indeed, the more security layers the IS professional had implemented across an enterprise, the more the individual exuded a calm, assured demeanor about their ability to anticipate and circumvent an attack. P1 and P6 cited fewer layers and were more likely to disclose reacting and remediating rather than anticipating and avoiding. Consequently, layered security coupled with training helps IS professionals prevent and minimize damage from social engineering attacks, which in turn gives a greater peace of mind concerning potential attacks.

Research question 2. "What is the essence of the shared experience of IS professionals in preventing social engineering vulnerabilities in U.S. businesses?" From five verbatim transcripts, 99 significant statements were extracted to address RQ2. Table 3 includes examples of significant statements with their derived meaning.

Table 3

Selected Examples of Significant Statements for RQ2

Significant Statement	Meaning
But you have to look at what you have accomplished, and so…. I think getting an involved with other IT professionals and getting networked--like going to [conference name] was a big deal, because you've got very sophisticated people wanting to figure out how you did it, right? So then it validates what you did. So, the company is never gonna understand, at large, what it took to get where you're at.	It feels good to have my work recognized and validated by others.
We probably weren't Tier 2 by then, but everybody's wearing many hats.	Preventing social engineering attacks is not my only job function--far from it!
There's gonna be a problem, right? If they don't stop working, then you don't stop working. So if they don't learn work-life bounds, then you can't have any as a security professional. Cause if the vice president's 24/, then his account's 24/7. If his account's 24/7, then phishing attempts are 24/7…	Sometimes working in this capacity is a 24/7 job, and that's difficult.
But at the end of the day, I have to play bad cop. All the time.	They want me to handle it rather than taking responsibility for their role.

Significant statements were then arranged into clusters, resulting in three themes. Table 4 contains examples of the theme clusters that emerged from their derived meanings.

Table 4

Theme Clusters with Related Derived Meaning for RQ2

Camping 101	Worker Bees	An Invisible Impact
Most of the time, social engineering attacks don't bother me.	Preventing social engineering attacks is not my only job function--far from it!	The work IS professionals do is hard to quantify.
IS professionals are frustrated by the poor decision-making of the people they try to protect.	IS professionals recognize their limitations and try to work around them.	I'm pleased with the security changes that have been made!
It can be difficult dealing with a team member.	Just my day-to-day role.	I'm proud of the work I do.
They want me to handle it rather than taking responsibility for their role.	People are the weakest link.	I'm proud of the work other IS professionals do.
Working as an IS professional isn't always fulfilling.	Sometimes other businesses and industries make it worse for my company.	It feels good to have my work recognized and validated by others in my industry.
The misuse of technology bothers me.		It feels good when my work is appreciated by my organization.

Theme 4: Camping 101. It seemed to be common knowledge among the participants in this study, if one hopes to operate a business without falling prey to a social engineering attack, an investment must be made to prevent the social engineering nuisance from ruining its chances for success. In truth, when asked to what extent social engineering attacks bothered them, none of the IS professionals confessed to spending much time bothered by them. In fact, both P2 and P3 admitted they only think about them "when they pop up." The other participants believed they had enough secondary security controls in place to neutralize the threat, so they were not bothered either. IS professionals in this study regarded social engineers like many campers treat the pesky mosquito—something that deserves enough attention to defend against, but not

necessarily something worth worrying about once controls have been put in place to protect the organization from an attack.

Theme 5: Worker bees. According to every participant, preventing social engineering vulnerabilities at their organization is not their only job function—far from it! Two participants, P2 and P3, estimated spending a minimal amount time (2% or less of their time) preventing social engineering vulnerabilities. The IS professionals working in security roles estimated that approximately half their time was spent working on cybersecurity tasks, with the prevention of social engineering tasks being lumped in with all other security-related activities. So what else are IS professionals doing? The participants in banking laughed heartily when posed this question, claiming, "Our hands are just about in everything." P1 also talked about wearing "many hats." Preventing social engineering attacks makes up only a fraction of work IS professionals do—even less when the role is not security-oriented.

Theme 6: An invisible impact. According to most participants in this study, because a lot of the work IS professionals do is behind the scenes, it often goes unnoticed by everyone else in the organization. And while they wholeheartedly believe their work is "impactful" to their organization, the work is also "hard to quantify." P1, a security professional, likened the work IS professionals do to "laying sewer pipe," explaining that "No one cares about the sewer pipe, but they do care that the toilet flushes." Essentially, the work IS professionals perform to defend their organization against social engineering attacks is not easy to measure or report on in terms of typical business objectives. So, even the social engineering or security risks faced by the company are considerably reduced, often there is no acknowledgement or reward for this significant achievement.

Research question 3. "What common meaning do IS professionals ascribe to the experiences of preventing social engineering vulnerabilities in U.S. businesses?" From five verbatim transcripts, 85 significant statements were extracted to address RQ3. Table 5 includes examples of significant statements with their derived meaning.

Table 5

Selected Examples of Significant Statements for RQ3

Significant Statement	Meaning
So, in a sense, everyone is responsible for preventing it. Obviously, we go through the training, you know, communicate--even if you didn't fall for it--we still got to communicate it to IT so they can let everybody else know, so nobody else falls for it. So, in a sense everyone.	Every person in the company is a steward of the company's data. Everybody is responsible for preventing SE attacks.
I believe that the amount of time that we devote to the function is--it corresponds to our size and complexity. I think if our size or complexity increases, then so will the resources that we--it's a direct--it's a proportional relationship.	Given our situation, the resources we direct towards preventing SE attacks is appropriate.
So I am--I am very pleased. Obviously, the banner was, I think, a genius idea. That--that's played a huge role, and just kind of, at least the internal--because that's what we were getting a lot of it first more so than the outward coming in type of attacks. It was, you know, someone posing as the CEO or someone posing as her husband or, you know, or as me or whatever. So that's been a hundred percent successful, in that case. And so, I'm very, very pleased with that.	Improving sometimes means making minor changes--that sometimes make a big impact!
[Policies and Procedures are] the way you live and die with security. It's extremely important.	The company lives and dies through their policies and procedures.
You'll never eliminate it. <<shakes head no>> You'll never eliminate it….. <<continues to shake head—direct eye contact>>	You can never eliminate all the risks.

Significant statements were then arranged into clusters, resulting in three themes. Table 6 contains examples of the theme clusters that emerged from their derived meanings.

Table 6

Theme Clusters with Related Derived Meaning for RQ3

To Protect and Serve	Harder, Better, Faster, Stronger	Risky Business
Every person in the company is a steward of the company's data.	Given our situation, the resources we direct towards preventing SE attacks is appropriate.	Training helps, but it's never going to be 100% effective.
Everybody is responsible for preventing SE attacks.	Improving sometimes means making minor changes--that sometimes make a big impact!	People are the weakest link and the greatest risk.
Protecting our company from SE attacks means protecting our reputation.	I'm proud of the improvements we've made to strengthen our company.	It actually helps a security culture when the people of an organization are a bit skeptical and don't trust.
Part of defending the organization is being an ambassador for security.	There will always be things we can improve.	You can never eliminate all the risks.
Finding ways to keep people accountable is an important step in keeping the organization safe.	We're continuously finding new ways to improve.	All our defenses cannot protect someone who doesn't protect themselves.
The experience/background of the IS professional makes a difference in how they address SE attacks.	You can never eliminate all the risks; you can only keep improving.	Policies and procedures help reduce risk, but they also cannot eliminate risk.

Theme 7: To protect and serve. Every participant in the study shared the belief that their role was to protect the organization and its stakeholders in whatever way their position and role allowed. Yet, they also all believed limitations existed on their ability to fully protect the company from social engineering attacks on their own. Each believed that every single person in the company is responsible for defending the organization against social engineering attacks, and they also shared that it was impossible to protect people who do not protect themselves. P1 called his role as an IS professional to be an "ambassador for security," and P3 called herself a "gatekeeper." As far as the people of the organization, participants shared the belief that people are "imperfect," the "weakest link," or the "greatest risk," but they are also the "stewards" of their organization's data in all their interactions inside and outside the organization. In sum, IS accepts their responsibility for protecting and defending the company from attacks, but they

cannot do it alone. Everyone at the company has a responsibility to defend the organization against social engineering attacks.

Theme 8: Harder, better, faster, stronger. Every participant in this study also credited continuous improvement as critical to successfully preventing social engineering vulnerabilities in U.S. businesses. Participants found intrinsic value in refining and improving the current situation at their workplace. P4 said, "I find value in what I do…. I see constant steps toward improvement, and I find reward in a continual process of improvement. We're better than we were yesterday. And tomorrow we'll be better than we are today." Likewise, P1, from the healthcare sector, after explaining how frustrating and difficult the challenge of improving the security defense at his startup had been, repeatedly emphasized, "It's much better now than it was." Continuous improvement, even minor advances, is integral to building a stronger defense against social engineering attacks.

Every participant in the study also shared the belief that that they were doing the best they could with the resources they had available at their workplace to address social engineering attacks. Multiple participants referenced the expectations of industry and regulatory standards as guiding them towards the appropriate levels of defense, stating that the primary goal is for an organization to be "doing your best at the size that you are." P4 added, "I believe that the amount of time that we devote to the function is--it corresponds to our size and complexity. I think if our size or complexity increases, then so will the resources." So, while not everyone has access to the same level of resources to defend an organization against social engineering attacks, most participants believed they are doing the best they can with the resources they have at their disposal.

Theme 9: Risky business. When considering the experience of preventing social engineering vulnerabilities in U.S. businesses, participants commonly ascribed their belief that one can never eliminate the potential risk of a social engineering attack as influencing why they continually strived to improve their defenses. Still, all agreed they still had the power to reduce risks. P4, the participant from banking who had previous experience working in the risk department, was most adamant in his assertion,

> The only way to eliminate risk is risk avoidance by not conducting the activity. <leans forward>> And the absence of activity creates no risk. Which is actually—it does create risk, because then you have the risk of not providing a product or service.

In attempting to reduce risks, participants again referenced the importance of communication, training, and education, as helpful, yet limited in that it could never be 100% effective. P3 attributed the existence of strong policies and procedures to forcing them to slow down "enough to where you had to think it through some more." Similarly, back in banking, P5 endorsed policies and procedures as "the way you live and die with security. It's extremely important." Because of the nature of social engineering attacks, it is common for IS professionals to believe the risk of an attack will never be fully eliminated, only minimized.

Research question 4. "What role do circumstances play in the methods chosen by IS professionals working in U.S. businesses to decrease security vulnerabilities related to human manipulation?" From five verbatim transcripts, 163 significant statements were extracted to address RQ4. Table 7 includes examples of significant statements with their derived meaning.

Table 7

Selected Examples of Significant Statements for RQ4

Significant Statement	Meaning
I got kicked in the deep end real quick. So, there was a lot of googling and a lot of calling professionals who … And my degree isn't even IT. My degree is in New Media and Marketing so--because I like being on the backend. I'm more of an introvert, so I didn't really want to work with people. I had been in retail. I was sick of people. I wanna go--get me an office or let me play with the equipment. And now you're running the help desk, and guess what you're dealing with people.	The factors and circumstances all interact with one another during the process of trying to decrease security vulnerabilities.
You know, we don't have escalation procedures, or policies and procedures, or committees that are going to review things.	How well defended an company is against attacks is dependent on the strength of the policies and procedures in place.
Annual audits—you know they look at that kinda stuff. And I go to all their classes, and they'll tell you all the different things they're gonna look at. And so we like to get a jump on that…	Availability of white papers and communication across an industry keeps IS professionals aware of potential risks and how they might be avoided.
And, that's kind of a common thing too, that I've heard with like banks of our size or, you know, smaller and community banks. So, they're hiring people, you know, like recruiting people not just from their community. You know, maybe they're outsourcing an information security officer…. Like outsourcing it.	A company's location may influence access to resources, including trained/experienced staff (sophisticated hiring pool).
Well, I think more heavily regulated, wouldn't you say? And so, I think that's part of it. Now, obviously, if we weren't, I mean people would still take the measures to be secure. But I think banks are way heavier regulated then even health care, and definitely schools!	The company's industry influences how much effort is expected by regulators to address security vulnerabilities.

Significant statements were then reviewed, resulting in one primary theme. Table 8 contains an example of the theme cluster that emerged from their derived meanings.

Table 8

Theme Clusters with Related Derived Meaning for RQ4

It's Not That Simple
These factors and circumstances all interact with one another during the process of trying to decrease security vulnerabilities.
As an organization matures, the methods used to decrease vulnerabilities change.
There are generational differences in employees, which influences how IS professionals communicate and train people about risks.
How well defended an org is against attacks is dependent on the strength of the policies and procedures in place.
The background/experience of an IS professional affects their decisions.

Theme 10: It's not that simple. It was clearly reported by all participants that circumstances made a difference in their ability to address social engineering attacks at their organization. Even so, responses also suggested a complex intermingling of factors rather than pointing to a single overriding condition or situation. For instance, P1 compared his experience of being a hired as an IS professional working for a small, rapidly growing startup in small town U.S.A. with that of a more mature organization.

> A mature organization--you've got a help desk. They've got a policy, procedure or, you know, you're probably on Enterprise Edition. You're pushing it all out from the top, you know? We can't spring for Enterprise Edition yet. We can't deploy things from a central location. We can't use a PXE boot server and create a Windows 10 boot file, right? We've got to stand up each machine with a person, and so that requires a person to go through their checklist. So, we're reviewing these all the time. We're still having to manage a staff that handles all the logistics--that hasn't been offloaded to Ops yet. We're doing all the ordering. All the procurement. All of that. Vendor relations so… I'm the only network engineer on staff. So, standing up a new VPN tunnel, or combine it--we're about to drop fiber and combine the networks--so we're doing that. We're reaching out to new security vendors, so vendor management. All those things are still IT management…. So, we have to be VOIP engineers. We're constantly moving accounts around. We have call center software that sits on top of that cues up calls, right? We have media dashboards that go out to the whole company, and how do you sync all that up? People call us and want to see statistics in real-time, and all of these things. Exchange administration--they all have email accounts. All of these things that other companies would be one job. You would have an exchange administrator. You would

> have an Active Directory administrator. And we have to do it all. It's me and two other guys. And so, we do all of that, and then, if there's time, we'll look at security. Yeah, you know, and so we've gotten SIM tools that help to automate, but you still have to have a human configure that.

Similarly, in higher education P3 conceded that being a state-funded institutional often meant "scrambling for pencils" due to the ongoing lack of funding, which leads to disputes about what the organization should spend those limited resources on. This, together with the lack of a designated person to spearhead the initiative, creates significant barriers to overcome. In contrast, participants from the banking sector believed they have been more successful at defending the organization for SE attacks primarily due to being "more heavily regulated" where they "have the FDIC or OCC come visit" on a "frequent" basis. The extensive level of oversight joined with being a mature organization with layered security, and ready access to financial resources and human capital, creates conditions that allow them to more thoroughly address social engineering attacks than experienced by the other participants in the study. Thus, it can be determined that the interaction of various factors creates complex, unique circumstances that each organization must operate within as they defend against social engineering attacks, and these circumstances can aid or hinder IS professionals as they determine the best way to address social engineering attacks given their current means and ability.

Evaluation of the Findings

The results of the study were primarily consistent with the body of literature presented in Section 1: Foundation of the Study section. Of the 10 themes derived for the study, seven were found to be consistent with the current body of literature. Three findings did not already appear to have been explored in the literature to date, and one of these appeared to be inconsistent with

what has already been written about the subject. Two subthemes also added new findings to the current body of research.

RQ1 themes. Three themes were derived for RQ1, "What lived experiences do IS professionals have with preventing social engineering vulnerabilities in U.S. businesses?" These themes include Theme 1: Security Cultivation, Theme 2: Train, Test, Repeat, and Theme 3: Layers, Not Just for Hair. Theme 1 was further subdivided into two subthemes, Subtheme 1: Find a partner, dosey doe and Subtheme 2: Tag! You're it. In the evaluation of each finding, all themes were found to be consistent with the body of literature.

Specifically, for Theme 1, the finding, whereby if an organization hopes to adequately defend itself from social engineering attacks its culture must allow and encourage its people to ask questions without penalty or chastisement, is consistent with Lineberry (2007) who establishes that effective information security is culturally ingrained across an organization. The finding from Theme 2, that to protect an organization from social engineering attacks all employees must be trained repeatedly to build awareness and withstand attacks is found strong support in studies by Campbell (2017), Peltier (2006), Dahbur et al. (2017), Bauer et al. (2017) and Torten et al. (2018). Last, Theme 3's finding, that layered security coupled with training helps IS professionals prevent and minimize damage from social engineering attacks is in line with multi-layered security program literature as discussed by Berti (2003), Chitrey et al. (2012), Conteh and Schmick (2016), and Amsden and Chen (2012).

RQ1 subthemes. Of the two subthemes for Theme 1, the first subtheme, which suggests a need to build strategic relationships is consistent with the study by Hagel (2014), who validated the importance of organizational leadership being on board and supporting the security culture. This first subtheme somewhat differs from Hagel's viewpoint, though, in that the participants in

the current study also found it necessary to form strategic relationships with people in non-leadership positions. Accordingly, this subtheme adds a new construct to the 2014 Hagel study. Additionally, the second subtheme for Theme 1, the finding that it is essential for an enterprise to designate someone with the responsibility of building and cultivating a stronger security culture is unique to the current study. More often, research designated the responsibility as a function of the security team or to information security workers in general (BLS OOS, 2018b), and, as a result, this finding builds on the body of literature that focuses on the role, function, and best practices of IS professionals attempting to defend their organization against social engineering attacks.

RQ2 themes. While all ten themes, when combined, capture the overall essence of the experience of the phenomenon, three themes were derived from participant interviews to directly address RQ2, "What is the essence of the shared experience of IS professionals in preventing social engineering vulnerabilities in U.S. businesses?" These themes include Theme 4: Camping 101, Theme 5: Worker Bees, and Theme 6: An Invisible Impact. Of the three themes described in this section, Theme 5, the finding that preventing social engineering attacks makes up only a fraction of work IS professionals do, is supported in the previous research surrounding work overload, occupational stress, and the IS worker (Agbonluae et al., 2017; Moore, 2000).

New findings. While previous research supports the need for investing in prevention and controls to reduce the threat of social engineering attacks (Brown, 2018; ISACA, 2016; Ponemon, 2017b), research does not yet appear to have identified the shared perspective of IS professionals presented in Themes 4 and 6. It should be noted that the perspective of IS professionals captured in Theme 4 seems to fall in opposition to that expressed in the literature.

Additionally, the finding in Theme 6 may offer additional insight into why some IS professionals experience higher levels of occupational stress and work exhaustion (Shih et al., 2013).

RQ3 themes. Three themes were derived for RQ3, "What common meaning do IS professionals ascribe to the experiences of preventing social engineering vulnerabilities in U.S. businesses?" These themes include Theme 7: To Protect and Serve, Theme 8: Harder, Faster, Better, Stronger, and Theme 9: Risky Businesses. Of the three findings for this RQ, Themes 7 and 8 were found to be consistent with the body of literature that recognized social engineering attacks as a problem everyone in the company needs to address (Mouton et al., 2016; Hagel, 2014; Proof Point, 2018; Huber et al., 2009; Indrajit, 2017; Mann, 2017) and that continuous improvement is integral to building a strong defense against social engineering attacks (Gardner &Thomas, 2014). The findings in Theme 8 were also consistent with the conceptual framework of the study, which touched on the importance of continuously improving to stay ahead of rapidly evolving social engineering attacks. The shared belief and perspective presented in Theme 9, that social engineering attacks can never be fully eliminated, is a finding that has not been previously noted in the literature.

RQ4 themes. One theme was derived for RQ4, "What role do circumstances play in the methods chosen by IS professionals working in U.S. businesses to decrease security vulnerabilities related to human manipulation?" This theme, Theme 10: It's Not That Simple, finds some consistency with the body of literature, which lends support to the added complexities encountered by IS professionals surrounded by the growing presence of cybercrime directed at the businesses (Amsden & Chen, 2012; Indrajit, 2017; Kshetri, 2006). Still, current research tends to focus on individual factors, like availability of financial resources or human capital (Brown, 2018; Moore, 2000; Poneman, 2017; Berti, 2003), and less social engineering

research has touched on the intermingling of factors and how these intertwined factors produce the decisions made by IS professionals to address social engineering vulnerabilities at their company. Many of the complexities discussed by participants aligned very closely with the types of information organizations use to determine the appropriate corporate and competitive strategy for their unique situation (Gamble et al., 2015).

Conceptual framework. Results of the study were also consistent with the conceptual framework presented in Section 1: Foundation of the Study. The framework consisted of four key parts: (a) anticipatory cybersecurity; (b) the social engineering defensive framework (SEDF); (c) beliefs, attitudes, and behavioral intention; and (d) occupational stress. The findings supported the role of anticipatory cybersecurity in allowing the business to offset social engineering attacks (Rege et al., 2017), but participants also recognized their current circumstances did not always make this ideal state feasible. In fact, only the participants from the banking sector appeared to have achieved this state.

SEDF. Still, while achieving a state of anticipatory cybersecurity was not always attainable, all participants utilized some form of continuous improvement, not unlike the SEDF continuous improvement cycle described by Gardner and Thomas (2014) to keep finding ways to become better. Although, when considering the four phases of the SEDF in light of the responses given by participants, much more emphasis was placed on the third phase, educating the workforce, than the other three phases (determine exposure, evaluate defenses, and streamline existing technology and policies). The framework appears to assume that companies are mature enough to have established and documented current policies, which was not necessarily the case with all participants in the current study. A few participants emphasized the

need to create technology and policies, but less was mentioned about streamlining existing technology and policies.

Beliefs, attitudes, and behavioral intentions. The findings fully supported the role of beliefs and attitudes in motivating the behavior of the participants in this study. Belief that the risk from social engineering attacks were real, scary and dangerous, but still avoidable motivated IS professionals to install controls and educate their workforce. Belief that they needed to improve the current situation for their organization led IS professionals to ask for funding, change their tactics to better sell the security culture, and push back or find creative solutions to the resistance to important security changes. Possessing an attitude that they were invested in the organization and responsible for its outcomes, inspired participants to accept their part in protecting the organization, learn from mistakes, and stimulate a stronger security culture.

Occupational stress. The findings in the study were also consistent with the research surrounding IS professionals and occupational stress, especially as they related to the high level of responsibilities and job demands placed upon these workers. Occupational stress continues to be a concern for some IS workers, as indicated by Agbonluae et al. (2017). Yet, while most participants admitted to being involved in "everything" or wearing "many hats," only one discussed feeling emotionally exhausted from the experience. Just as Moore pointed out in his 2000 study, this participant believed his work overload partially stemmed from the inadequate staff and deficient resources available to him at his workplace.

Triangulation. Triangulation was achieved in the research process in three steps. First, the researcher's point of view was captured during a self-reflection journaling process, whereby the researcher used the research questions and interview questions as guided journal prompts, responding with her thoughts, personal experiences, beliefs and biases. Second, the researcher

gathered evidence from study participants through the interview process. As will be seen in the following section, study participants came from three distinct industries, across various IS functions. Each had unique backgrounds and lived experiences that were collected and transcribed, then analyzed, coded, and compared. Additionally, verbatim transcriptions were shared with participants, and member checking was used to validate the transcript for accuracy. The third step of the triangulation process is the presentation of the findings to readers of the study. According to Creswell and Poth (2018), to complete triangulation, the description of the phenomenon allows readers of the study to visualize whether the findings might be applied, or transferred, to other situations. Thus, triangulation has been addressed in this study by capturing and presenting the points of views of the researcher, participants, and readers.

Saturation. According to van Manen (2016), data saturation in phenomenological studies depends on having enough "experientially rich accounts" (p. 353) to sufficiently present the essence of the phenomenon to readers. The researcher realized saturation had been reached after significant statements had been extracted to enable the researcher to address each RQ and write a rich description of the essence of the phenomenon, as experienced by the participants. In all, five interviews were conducted with six participants, where two participants (a male and female) from each industry were represented in the study. The data analysis process was completed after five in-depth interviews, which is when the researcher determined the ten themes and subthemes fully captured the experiences of IS professionals defending their organization against social engineering attacks.

Analysis and Implications

This phenomenological study was designed to discover what the shared experience of IS professionals defending their organization against social engineering attacks is like. What has

been presented is the experiences of the study participants, rather than the interpretations of the researcher. This section consists of the analysis and implications of the findings, which will conclude with a summary of the essence of the phenomenon.

Analysis of RQ1 findings. Results of RQ1 were assimilated into an overall framework of the lived experience of IS professionals working to prevent social engineering attacks on their organization. The combined themes indicate that, initially, the lived experience begins with establishing a security culture by opening lines of communication and building strategic relationships inside and outside of the organization. From there, IS professionals utilize whatever resources they have at their disposal to spread awareness of social engineering attacks and the role each person plays in preventing these attacks throughout the company. IS professionals accomplish this through regular, repeated testing. Lastly, IS professionals recognize they are operating within certain constraints. For instance, no matter how often employees receive training, humans remain the weakest human link in the security chain. For that reason, they seek to protect the organization using layered controls in hopes that if one or more layer of security is penetrated, another layer will catch and eliminate the threat. Even so, the need for stronger controls and situational constraints have pushed IS professionals to investigate and leverage outsourcing opportunities to enhance their security layers beyond what they could otherwise do themselves.

Implications of RQ1 findings. Stakeholders stand to benefit from these findings through increased investigations into the differences between those who have created a stronger security culture and those who struggle to do so. The findings also provide guidance IS professionals attempting to change or improve their current culture, including taking special care to address communication issues, build strategic relationships, and designate a primary person

with the responsibility of managing all aspects of information security. The second finding, Theme 2, informs stakeholders of the need for ongoing, consistent, and repetitive training to build a stronger defense against social engineering attacks. This finding presents the opportunity for IS professionals and researchers not only to invest in more social engineering-related training materials, but also to find ways to more readily disseminate and share materials among all businesses and IS professionals. The third theme and final finding of RQ1 recognizes that while training is important, it will never be enough. This finding lends support to the installation of as many layers of controls as within the means of the organization, so that when an attack breaches the initial line of defense, the subsequent layers of electronic controls will catch it before it does further damage.

Analysis of RQ2 findings. The combined themes, Theme 4: Camping 101, Theme 5: Worker Bees, and Theme 6: An Invisible Impact, flow together to form the core of the essence of the experience of IS professionals working to defend an organization against social engineering attacks. The findings from this section offer key insights into how social engineering attacks are viewed by IS professionals operating in U.S. businesses--pesky, yet unavoidable. Feelings about this phenomenon fluctuated between "frustrating," "annoying," and "difficult" to feeling "lucky" they were in the right place at the right time to quickly remediate an attack. While not every participant claimed to spend a significant amount of time defending their organization against social engineering attacks, each accepted that they played some part. Also, participants admitted to wearing "many hats" and having an active role "in every department," stating "there's pretty much nothing we don't do."

Finally, even though they were actively involved in "just about everything," often, the progress made by IS professionals to secure and protect the organization goes unnoticed or

unrecognized by leadership because it can only be quantified when something bad happens. Participants in this study acknowledged that validation for their work protecting the organization usually comes from a sense of internal pride from looking back over their accomplishments to seek how far they have come, knowing that everything is working, or being recognized by external peers who understand how "thankless" it can be when "laying sewer pipe." While some participants in this study were more inclined to avoid the "limelight," others found themselves battling "depression and anxiety" stemming from the working conditions coupled with the fact that "nobody cares."

Implications of RQ2 findings. These findings shed light on the fact that IS professionals are extremely busy workers who rely on everyone in their company to help with the defense against social engineering attacks. Understanding the need and frustrations that result from attempting to have everyone on board may help more stakeholders recognize their personal role and contribution to protecting the company, which in turn, could strengthen the overall defense of the organization. These findings are also significant, because they shed light on a potential need to find better ways to quantify the work that security professionals do. Finding ways to better support IS professionals by recognizing their value and contribution to the success of the organization may help to combat some of the negative feelings when experience work overload.

Analysis of RQ3 findings. IS professionals were clear—they cannot protect the organization alone. And all the training, electronic controls, policies and procedures, resources, another other defenses cannot help people who will not help or change themselves. All participants acknowledged that everyone--from the top of the organization to the bottom, across to customers and vendors--is responsible for protecting the organization from social engineering

attacks. Each participant felt they were doing the best they can at their current level of resources. Still, seeking new ways to improve and get better—to make the lives of everyone around them better—is also a way of life for the IS professionals in this study. Like the use of the SEDF by Gardner and Thomas (2014), every participant sought ways to improve their current level of defense against social engineering attacks within the scope of there IS role and function. Indeed, some of their frustrations stemmed directly from the resistance they received from the very same people they were attempting to make life easier on. They nearly all agreed that it was impossible to eliminate risk, but working together with their various stakeholders, significant progress could minimize the threat. It should be noted that in most cases, it seemed this perspective, that risk was impossible to eliminate, drove the need to continuously find better way to improve and enhance their defenses as they strived to stay ahead of the curve as the participants responded social engineering threats.

Implications of RQ3 findings. The findings for RQ3 are important, because it recognizes the limitations places on IS professionals in this phenomenon. IS professionals are fully dependent on everyone else being aware of potential attacks in the moment, not sharing passwords, and not clicking on questionable links. They have no control in these areas. While IS workers might install more controls, some may be limited by financial resources or manpower. Understanding it is important to train or guide actions, but not every IS professional has time to write the training materials or document their policies and procedures in addition to their other ongoing IS duties. Moreover, even if IS professionals communicate and train, they may be limited by resistance to changing the way things have already been done. There will always be limitations for IS professionals striving for a more secure organization. Still, it is important for IS professionals to understand that others have faced similar circumstances and

have made their situation better by leaning on the incremental improvement process, rolling out changes bit by bit. If it can happen at one organization, it can happen at another.

Analysis of RQ4 findings. In addressing RQ4, it was clear that all participants believed the circumstances they found themselves in influenced their ability to defend their organization against social engineering attacks, and that these beliefs and attitudes motivated their behaviors, as described by Fishbein and Ajzen (1975) in the conceptual framework. It was much less clear how much one factor, such as role, resources, background/experience, or industry expectations, contributed to their overall ability to defend against such attacks. As the only theme for RQ4 suggests, the responses of the participants indicate that multiple, interwoven factors are at play when IS professionals consider the best ways to protect their company from social engineering attacks, and with so many factors interacting at once, solving one problem may result in a dilemma, where other areas are negatively affected even though one issue might be resolved (Bergquist & Mura, 2011).

Implications of RQ4 findings. These findings are important to stakeholders because not every decision related to defending an organization against social engineering attacks is cut and dry. This finding is key to understanding why some IS professionals successfully anticipate and plug security vulnerabilities while others struggle to react and remediate fast enough, as discussed in the conceptual framework. Not having a clear cut, easy solution that does not negatively affect other parts of the organization makes decision-making more difficult, and difficult decisions take time to resolve. Still research has been shown to help investigators understand and predict the behaviors of people, which could provide further insights into the phenomenon (Ajzen, 1991).

Summary of the Analysis

According to participants, the lived experience of protecting an organization against social engineering attacks involves unifying all the people of an organization to work together by employing open communication, continuous education and testing, and strong policies and procedures, coupled with an amalgamation of layered technology and electronic controls. At the heart of the shared experience is the acknowledgement by participants that social engineering attacks are unavoidable, the risk of a social engineering attack will never be eliminated and IS professionals cannot protect the organization and the people of the organization alone. Moreover, participants voiced that entwined factors, including maturity, location, resources, manpower, experience, regulations, and industry, also influenced the circumstances and limited their ability to address their social engineering vulnerabilities at any given moment. Consequently, it is more difficult for some IS professionals to deal with social engineering attacks using the more effective anticipatory approach (Rege et al., 2017). Nonetheless, participants also shared the desire and drive to keep improving and making the situation better, often finding success in the incremental improvement process, such as the described in Gardner and Thomas' (2014) SEDF.

Understanding the lived experiences of IS professionals for the current phenomenon is important for stakeholders seeking to prepare a stronger, anticipatory defense against social engineering attacks at their organization, because establishing a strong defense system is not a straightforward task. The new complications can increase the already existing occupational stressors that stem from an already significant level of responsibilities often experienced by IS professionals (Messersmith, 2007). Not considering the significance of the work involved to better protect an organization against social engineering vulnerabilities, could potentially lead to

overwork and emotional exhaustion, which has been linked to reduced worker productivity (Donald et al., 2005). Furthermore, recognizing what other IS professionals have already experienced can help a stakeholder to better prepare for some of the frustrations that have already been encountered by others, possibly helping them to avoid potential pitfalls by learning from someone else.

It is also important for stakeholders to consider the beliefs and attitudes in comparison with their own beliefs and attitudes, as human behaviors can be predicted by attitudes and behavioral intentions (Ajzen, 1991). For instance, knowing that participants believe that social engineering risks will never be eliminated and that IS professionals cannot tackle the issue alone is important for stakeholders to understand that defense entails a culture change, which must start at the top and trickle down. Consequently, because shared beliefs and attitudes point to predictable actions and patterns (Fishbein & Ajzen, 1975; Ajzen, 1991), practitioners can seek out the actions and patterns of those with similar beliefs and use their results to learn and improve upon.

Finally, it also helps for stakeholders to understand that much of the work that IS professionals do is hard to quantify, invisible unless something goes wrong. Stakeholders who understand this quality of IS work can seek better ways to acknowledge, support, and quantify the work of IS professionals. Addressing this issue has the potential to produce positive results for the morale of the IS function, which can have positive benefits the organization at large, as discussed in the occupational stress research conducted with IS workers (Moore, 2000; Donald et al., 2005; Johnson & Hall, 1988; Karasek, 1979; Karasek & Theorell, 1990; Salanova et al., 2002; Moen et al., 2016).

Applications to Professional Practice

This last section addresses how the findings of the study are applicable to business and industry. First, the recommendations for action are presented. Next, the recommendations for further study are considered. Third, reflections on the researcher's experience throughout the research process are discussed. Finally, the section concludes with a summary and study conclusions.

Recommendations for action. Primarily, it is expected that the results may offer relevant insights and applicable recommendations to IS professionals and organizational leadership. The conclusions may also be applicable to HR professionals, or those responsible for the training and education activities of the organization. Any organizations or industries that currently consider themselves to be highly vulnerable to social engineering attacks may also benefit from the recommended actions and insights disclosed in this section. Recommendations also address the role of educators, consultants, vendors, and researchers, calling them to action in tackling the dearth of widely available training materials. All these groups, as well as students, may be impacted by the results of this study.

Designated IS security personnel. The findings indicate a need for every organization to designate someone with the responsibility of dealing with information security, which includes preventing social engineering attacks building a stronger security culture. It is recommended that business and IS leadership take a closer look at the current situation to determine if it is possible to create such a position. For those unable to create a new position or hire new personnel to fill that role for the company, then it is recommended for these persons to determine whether outsourcing might help relieve certain duties or to investigate whether current responsibilities and staff might be reorganized to fill this need.

Incremental improvements. In terms of things IS professionals are already doing right, the findings support the continued use of continuous improvement processes to strengthen the defenses of the organizations. For the most part, the recommendation is for IS professionals engaging in these continuous improvement activities to keep doing what they are doing, only to focus additional efforts towards reducing areas most vulnerable to social engineering attacks. For IS professionals struggling to improve given their current level of resources or situational circumstances, it is recommended for them to investigate how other IS professionals in their industry are using continuous improvement processes to defend against social engineering attacks to determine if some of these activities can be applied to their situation.

Establish training partnerships. The findings indicate that prevention of social engineering attacks is heavily reliant on training, an activity not all organizations can create themselves. It is recommended that educators, vendors, and consultants seek out and invest in opportunities to create and offer training materials and seminars that can be used by any company operating in any industry, possibly developing a repository of training materials that can help organizations with fewer resources gain access to tools that will help them strengthen their defense. It is also suggested that organizations and IS leadership seek to partner with these persons or groups to determine the best and most effective training methods for everyone.

Spread awareness. As shown in the Camping 101 theme, it is now understood that anyone operating or engaged in business in the U.S. is at risk to be attacked by a social engineer. The question is no longer *if*, but *when*. Thus, it is recommended for educators at all levels where technology and the Internet are being used to accomplish class-related tasks, to incorporate social engineering awareness and prevention throughout the curriculum. This is especially relevant for

educators of business and CIS instructors in postsecondary institutions, as these are the future leaders and employees of U.S. businesses.

Educators might accomplish this through an initial introduction of the topic prior to using any new technology or tool with online capabilities. It is recommended that educators engage business practitioners as guest lecturers who can clearly describe the risks that social engineering poses to students and their families. It is also suggested that the educators follow up with handouts and hands-on assignments, potentially incorporating a testing component. For students in elementary through secondary school, it is recommended that additional training sessions be held with parents to ensure they understand their role in protecting the student and themselves from the risks of social engineering attacks that could occur using these devices. Informational handouts discussing the risks and ways to prevent social engineering attacks should be shared directly with parents whose children will be using technology during the school year. Furthermore, it is recommended that a section be dedicated to the prevention of social engineering attacks the policies and procedures handbook for students, parents, and faculty.

Require minimum social engineering training. Across all industries, it is recommended that new employees receive, at a minimum, an initial introductory course to social engineering and the risks they pose to the organization. The training should be included with typical HR new hire training, whereby employees are made aware of the expectations of the organization regarding how an employee should be aware of the risk and how to act if they suspect an attack attempt. It is also recommended for organizations to require employees, especially those with access to the Internet, social networks, email, and company networks, to participate in an annual or biennial refresher course, depending on the role of the employee and the risk they pose to the organization, should they be targeted by a social engineer. While the primary group affected by

this recommendation is the HR staff, as they may be required to invest in or create the training materials in addition to leading the training sessions, it is also recommended for the IS team to be involved in this process to ensure new employees know the process of who to call and how to communicate with the IS team in case of an incident.

Additional testing. For companies with access to greater resources, additional testing or interactive learning opportunities are recommended to cement the learning process for employees. For those with access to fewer resources, finding additional ways to keep the risk in the forefront of employee minds, such as quarterly email reminders or lunch and learn professional development opportunities, may be more applicable and cost-effective solutions. A final recommendation for those seeking lower-budget solutions to spread more awareness about social engineering would be to investigate outside assistance from educators or even students and interns attempting to build their skills and proficiencies through experiential or service-learning. Allowing them to develop the training materials and lead the training sessions enables both the business and student to partner together to achieve their goals.

Sharing is caring. Participants in this study believed in the importance of learning and growing from their experiences after having experienced a social engineering attack. Communication with employees, venders, and other IS professionals was considered key to this learning process. Participants signed up for email newsfeeds related to industry cyberattacks, and they used the information shared in these messages to plug holes they were not initially aware were an issue. Others attending meetings or conferences and spoke with vendors, customers, and even auditors. From each encounter, participants gleaned more from other's experiences and close encounters and found new ideas to improve their own circumstances. To this end, it is recommended for IS professionals to seek as many opportunities to talk with one

another and share their experiences openly with one another and with the employees across their company using various dissemination methods, such as email, lunch and learns, targeted training sessions, departmental visitations, Q&A sessions, conferences, and more.

Stronger policies and procedures. Participants confirmed that stronger policies and procedures was essential to cultivating a strong defensive stance against social engineering attacks. Accordingly, the final recommendation to action is for IS professionals to carefully review current policies and procedures related to social engineering across their organization. IS professionals should compare internal policies and procedures against the standards found not only within the industry they operate, but also across other industries, giving special notice to the policies and procedures required by industries with the highest regulatory requirements. Once the comparison is complete, IS professionals are encouraged to any adopt best practices, policies, and procedures that lie within their current level of resources and capability, taking note of any out of reach that might be implemented at a future date. Last, it is advised that IS professionals include the review and update of social engineering policies and procedures as part of their ongoing continuous improvement processes.

Recommendations for further study. In terms of future research opportunities, it is important to recognize the limitations of the current study. The study was centered on three industries in a very narrow geographic region, specifically, the central to northwest regions of Louisiana. Participants were primarily from small and medium sized businesses located in rural communities. Consequently, the voices of participants this study may not accurately reflect the voices of those persons working at larger companies located in more populated, metropolitan regions or states. Hence, opportunities exist to replicate the study in other regions and states to see if the findings are consistent in other industries and for a group of participants not included in

the current study. It would be interesting to see a study targeting larger, more mature enterprises with access to greater resources to determine if the findings remain consistent.

Qualitative phenomenological inquiry. This study was qualitative in nature, with the goal of understanding the experience of IS professionals as they defend their organization from social engineering attacks. Every inquiry style comes with its own limitations. For instance, the current phenomenological study is limited by its inability to determine if relationships exist between some of the variables identified in the study. This could be addressed in future research using a quantitative or mixed methods methodology. Unlike grounded theory studies, which is characterized by the generation of a theory (Strauss & Corbin, 1997; Stake, 2010), phenomenological studies primarily seek to understand what a shared phenomenon is like. A next logical step following this study might be to use a grounded theory approach to look more closely at the data to discover a theory about the shared experience of IS professionals in this phenomenon. Thus, it is recommended that future researchers build on the results of the current study by determine which other research lens will offer greater insights to the experience of IS professionals defending their organization against social engineering attacks.

Attitudes are everything. It is also recommended for researchers to perform a nationwide mixed methods survey focused on widespread believes and attitudes of business professionals towards social engineering and cyber security attacks at large. Research could focus solely on IS professionals, business professionals, or on comparing the beliefs and attitudes between IS and business professionals. Some of these thoughts, beliefs, and attitudes are currently captured across the annual cybersecurity surveys (Ponemon, 2017b; Proof Point, 2018; IBM, 2016; IDG, 2015), but the further research should determine how common these beliefs and attitudes exist and why IS professionals hold these beliefs. To accomplish this, a researcher would need to

develop a synthesized, comprehensive list of beliefs and attitudes from current studies and develop a survey to administer to practitioners. Additionally, because beliefs, attitudes, and behavioral intention can predict behavioral actions, it is recommended for researchers to seek out links between these beliefs, attitudes, and behavioral patterns. A study like this may offer additional insights to researchers and practitioners trying to better understand the phenomenon.

Social engineering prevention focus. Participants in the study indicated that training is everything to prevention, and that not every organization had the same level of access to the materials needed to prevent an attack. Indeed, at least one participant was responsible for writing their own training material. To better help businesses with limited resources and access to social engineering training materials, it is recommended for researchers to investigate what training materials dedicated to social engineering prevention presently exists, and to what extent these materials are available across all business and industries.

Establishing a security culture. Participants described the difficulties encountered as they attempted to transition from a non-security culture to a security-minded culture. Understanding what the experience is like as they make this transition may help businesses better steer through the potential landmines that have been encountered by their sister enterprises. To accomplish this, a phenomenological study investigating the experience of IS professionals as they lead an organization through this transition would be recommended to help capture and understand the lived experiences of IS professionals navigating this transition.

Who is at the helm? In addition, because the findings indicate the importance of having a designated security person leading the transition from insecure to secure against social engineering vulnerabilities, a mixed methods study investigating how many organizations currently employ a dedicated IS information security lead. During this investigation, it is

recommended for the researcher to examine the differences between companies with and without dedicated personnel in terms of the level of defenses in place. The study should discuss the level and quality of training and prevention activities as well as electronic controls.

Reflections. In tackling this project, the researcher attempted to extract personal biases by bracketing these into an epoche, presented earlier in the study. To accomplish this task, the researcher used the research and interview questions as journal prompts, in which she responded with her personal thoughts, feelings, beliefs, and personal experiences. In doing so, this allowed the researcher to approach each interview with an openness and desire to hear to the voices of the participants rather than to push forth her own views. Still, the researcher experienced moments during every interview where her personal experiences and viewpoints were either challenged or completely unraveled.

Additionally, the researcher discovered after conducting the first interviews, she had unexpectedly adopted some of the attitudes, beliefs, and biases of previous participants, as she found her seeking similar experiences with subsequent participants. Again, the researcher found herself impressed when, yet again, these adopted notions and biases were challenged by the latest participant. Upon further reflection, even though the researcher was initially concerned that her biases may have inadvertently influenced the participants, she was also pleased that participants felt comfortable enough with her and the interview process to immediately correct any inaccurate or biased statements that did not align with their lived experience. This demonstrated to the researcher that participants accepted their responsibility to honestly and accurately convey their true experiences, rather than simply to accept and confirm those presented to them. Next, the researcher reflects on the key insights and takeaways from the research process.

Overwhelmed? Not so much. The responses from participants were not in line with what the researcher initially expected to receive. For instance, the researcher expected that more participants would share feelings of overwhelm and overwork in relation to their ability to address social engineering attacks in additional to the other takes they were juggling daily. Of the six participants, only one expressed these types of feelings, but he also fully admitted that his experience could easily stem from the constant changes experienced by an IS professionals working for a rapidly growing startup. A few participants expressed a sincere appreciation for their company and the people they work with. Most appeared invested and content, rather than overworked and overwhelmed.

Menace, indeed. The researcher also initially believed, after reading the alarming portrayal of social engineering and cyber-attacks in the literature, that participants would be more disturbed by social engineering attacks and the risks they posed to their organization. Given the terrifying portrayal of this menace in the body of research, the investigator was completely taken aback by the unruffled responses indicating they had accepted social engineering attacks were simply a fact of life. But then, after further reflection, perhaps it should not have been so surprising that none of the participants had time to sit around and worry about social engineering attacks, given the varied roles and the significant amount of responsibility each juggled regularly.

Unexpected need. The need for a dedicated IS staff person to be designated with the responsibility of building the security culture for an organization was not the researcher's radar as important until she spoke with a participant who worked for an organization that did not have someone designated with this responsibility. In fact, it was the stark contrast between how participants without a dedicated team member responded to interview questions as compared to

those who worked for organization with dedicated IS security personnel that enabled the researcher to identify this significant insight. Those participants with dedicated security personnel appeared better prepared to defend against social engineering attacks than those without. Had the study failed to include an industry like higher education, this key finding might have gone unnoticed, because each participant working for businesses with a dedicated IS security person approached this type of position as an implied expectation for their organization. Only those participants from higher education could offer the salient insight and perspective of what organizations experience when no one is assigned to this role.

More policies and procedures? Oh my. Prior to conducting the current study, the researcher fully acknowledges having negative biases about the role of policies and procedures in the workplace. She was also unaware that this bias would be challenged by the majority participants in terms of being relevant to the prevention of social engineering attacks on U.S. businesses. In fact, this bias was excluded from any of the thoughts and beliefs the researcher wrote about as she bracketed out her experiences, simply because she was unconscious of the significance of policies and procedures to the security culture and posture of a company. After hearing the unified chorus of participant voices, the researcher is now able to fully appreciate how well-constructed and implemented policies and procedures help protect the organization, including its assets, employees, and stakeholders.

Biblical principles. In reflecting on the implications for biblical practice previously discussed in Section 1, the researcher concedes that the research process, specifically engaging with the participants, allowed her to expand her original perspective beyond the need to simply highlight the efforts of IS professionals. To conclude this section is a quote shared by a participant about the meaning he found in his work to protect his company from social

engineering attacks. The quote is a reminder of how people are image bearers of God (Keller & Alsdorf, 2012). The analogy reveals a beautiful illustration of how God is reflected in the work of IS professionals.

> There's an episode of Futurama. Where Bender gets lost and he meets God--or what we expect was God, right? The quote is, 'When you do everything right, people won't be sure you've done anything at all.' So that's *very* pertinent to security and IT. When everything is working the way it should. They'll start to question why they're even paying you. Which is a battle you're gonna fight. But that's--that's the meaning you have to get out of it. I can sit back and have a beer and it's all just working. And no one knows what it took.

Summary and Study Conclusions

In conclusion, the current study investigated the problem that U.S. businesses remain vulnerable to costly social engineering attacks. The specific problem addressed by this study was the deficient understanding about how IS professionals make sense of their lives and experiences as they address and prevent weaknesses related to social engineering attacks while working in businesses within the healthcare, financial services, and higher education industries across central and northwest regions of Louisiana. The study sought to understand how IS professionals working in U.S. businesses make sense of their lives and experiences as they address and prevent vulnerabilities to social engineering attacks.

Because establishing a strong posture against social engineering attacks involves a complex interaction of factors, understanding this phenomenon is important for all stakeholders attempting to strengthen their defenses against social engineering threats. The study offers recommendations to IS professionals, business leadership, HR professionals, educators,

consultants, vendors, and researchers in addressing issues related to designating a dedicated IS security team member, continuing to focus on incremental improvements, establishing training partnerships, spreading awareness, requiring minimum social engineering training expectations, sharing and communicating about vulnerabilities, and installing stronger policies and procedures. Also presented are areas recommended for further study, including additional qualitative phenomenological inquiries, mixed method investigations into differences between the beliefs and attitudes of IS professionals and businesses professionals about social engineering, closer examinations of the available social engineering prevention research, and studies investigating the experience of IS professionals as they transition from an insecure culture to a security-minded culture.

The topic of social engineering has achieved academic significance, as seen in the increased interest in the number of social engineering research papers published in recent years (Zheng, Wu, Wang, Wu, & Wu, 2019). By adhering to a qualitative research approach, the current study bridged a gap in the social engineering literature, which was primarily comprised of studies that utilized a quantitative methodology. The present study adds to the body of literature through its use of a phenomenological research design. Prior to this investigation, the body of literature did not include a phenomenological study that focused on capturing the essence of the lived experience of IS professionals as they protect their company from social engineering attacks. Lastly, the literature lacked information about the shared attitudes, beliefs, and motivations of IS professionals as they experienced this phenomenon. The use of a qualitative approach allowed participants to give voice to their beliefs, thoughts, and motivations about the work they do in this regard.

The inquiry involved six participants who identified themselves as IS professionals working in businesses in central and northwest Louisiana. Each participant had experiences addressing and preventing social engineering vulnerabilities at their workplace. The results of the study consisted of ten themes and two subthemes, which were derived from the transcription, analysis, and coding of the in-depth interviews with the six participants. Together, these themes and subthemes capture the overall essence of the lived experiences of the phenomenon. The themes include Theme 1: Security Cultivation, Theme 2: Train, Test, Repeat, Theme 3: Layers, Not Just for Hair, Theme 4: Camping 101, Theme 5: Worker Bees, Theme 6: An Invisible Impact, Theme 7: To Protect and Serve, Theme 8: Harder, Better, Faster, Stronger, Theme 9: Risky Business, and Theme 10: It's Not That Simple. The two subthemes of Theme 1 included Subtheme 1: Find a Partner, Dosey Doe and Subtheme 2: Tag! You're It.

The findings revealed that the lived experience of protecting an organization from social engineering attacks involves the unification of people across the enterprise to develop a strong security-minded culture. This is accomplished by establishing open communication with the IS professionals and other employees of the business, continuously engaging employees in social engineering education and training. The culture is also supported by strong, clear policies and procedures and layers of technology and electronic controls. Participants shared two primary beliefs (a) that social engineering attacks would never be eradicated and (b) IS professionals depend on everyone in the organization to protect the organization from social engineering attacks. They cannot do it alone.

References

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Santa Monica, CA: Rand Corporation.

Agbonluae, O. O., Omi-Ujuanbi, G. O., & Akpede, M. (2017). Coping strategies for managing occupational stress for improved worker productivity. *IFE PsychologIA: An International Journal*, *25*(2), 300-309.

Airehrour, D., Nisha, V. N., & Madanian, S. (2018). Social engineering attacks and countermeasures in the New Zealand banking system: Advancing a user-reflective mitigation model. *Information*, *9*(5), 110. doi:10.3390/info9050110

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, *8*(1), 1-24. doi:10.1186/s13673-018-0128-7

Amsden, N. D., & Chen, L. (2012, January). Combating social engineering: A DoD perspective. In *Proceedings of the International Conference on Security and Management* (SAM; p. 1). The Steering Committee of the World Congress in Computer Science, Computer Engineering, and Applied Computering (WorldComp). Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com .ezproxy.liberty.edu/docview/1426803183?accountid=12085

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, *22*(4), 308-313.

Anderson, P. C. (2017). Cyber-attack exception to the foreign sovereign immunities act. *Cornell Law Review*, *102*(4), 1087.

Applegate, S. D. (2009). Social engineering: Hacking the wetware! *Information Security Journal: A Global Perspective*, *18*(1), 40-46. doi:10.1080/19393550802623214

Armstrong, D. J., Brooks, N., & Riemenschneider, C. K. (2015). Exhaustion from information system career experience: Implications for turn-away intention. *MIS Quarterly*, *39*(3), 713-727. doi:10.25300/MISQ/2015/39.3.10

Axelos. (2016, May). Cyber Resilience: Are your people your most effective defense? *Axelos*. Retrieved from www.axelos.com/Corporate/media/Files/RESILIA_Report-16.pdf

Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social engineering: Assessing vulnerabilities in practice. *Information Management & Computer Security*, *17*(1), 53-63. doi:10.1108/09685220910944768

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145-159. doi:10.1016/j.cose.2017.04.009

Bere, M., Bhunu-Shava, F., Gamundani, A., & Nhamu, I. (2015). How advanced persistent threats exploit humans. *International Journal of Computer Science Issues (IJCSI)*, *12*(6), 170-174.

Bergquist, W., & Mura, A. (2011). *Coachbook: A guide to organizational coaching strategies and practices*. Seattle, WA: CreateSpace Independent Publishing Platform.

Berti, J. (2003). Social engineering: The forgotten risk. *Canadian HR Reporter*, *16*(13), 21-21,23.

Brown, T. (2018). Are miserly budgets putting businesses at risk of cyber-attack? *Computer Fraud & Security*, *2018*(8), 9-11. doi:10.1016/S1361-3723(18)30074-5

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory*, *6*(3), 203-242.

Buller, D. B., Burgoon, J. K., Buslig, A., & Roiger, J. (1996). Testing interpersonal deception theory: The language of interpersonal deception. *Communication Theory*, *6*(3), 268-288.

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security*, *2016*(6), 8-14. doi:10.1016/S1361-3723(15)30046-4

Campbell, C. (2017). *Exploring future solutions to counter social engineering attacks: A Delphi study* (Order No. 10285134). Available from ProQuest Dissertations & Theses Global. (1917010266). Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu/docview/1917010266?accountid=12085

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, *12*(1), 28-38. doi:10.1109/MSP.2013.106

Carlton, M. (2016). *Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills* (Order No. 10240271). Available from ProQuest Dissertations & Theses Global. (1834580233). Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com .ezproxy.liberty.edu/docview/1834580233?accountid=12085

Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701-15. doi:10.1007/s11948-014-9551-y

Chilton, M. A., Hardgrave, B. C., & Armstrong, D. J. (2010). Performance and strain levels of IT workers engaged in rapidly changing environments: A person-job fit perspective. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *41*(1), 8-35.

Chitrey, A., Singh, D., & Singh, V. (2012). A comprehensive study of social engineering-based attacks in India to develop a conceptual model. *International Journal of Information and Network Security*, *1*(2), 45. doi:10.11591/ijins.v1i2.426

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology*, *55*, 591-621.

Clandinin, D. J. (2016). *Engaging in narrative inquiry*. New York, NY: Routledge.

Clandinin, D., & Caine, V. (2008). Narrative Inquiry. *In* L. M. Given (Ed.), *The Sage Encyclopedia of Qualitative Research Methods* (pp. 542-545). Thousand Oaks, CA: Sage. doi:10.4135/9781412963909.n275

Colomo-Palacios, R., Casado-Lumbreras, C., Soto-Acosta, P., GarcíA-PeñAlvo, F. J., & Tovar-Caro, E. (2013). Competence gaps in software personnel: A multi-organizational study. *Computers in Human Behavior*, *29*(2), 456-461.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31-38. doi:10.19101/IJACR.2016.623006

Cox, J. (2012). Information systems user security: A structured model of the knowing doing gap. *Computers in Human Behavior*, *28*(5), 1849-1858.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13-21. doi:10.22215/timreview835

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: Sage.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (4th ed.). Thousand Oaks, CA: Sage.

Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). Assessment of security awareness: A qualitative and quantitative study. *International Management Review*, *13*(1), 37-58,101-102.

Davis, P. K. (2014). Deterrence, influence, cyberattack, and cyberwar. *New York University Journal of International Law and Politics*, *47*(2), 327.

Demchenko, Y., Zhao, Z., Grosso, P., Wibisono, A., & De Laat, C. (2012, December). Addressing big data challenges for scientific data infrastructure. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on* (pp. 614-617). IEEE. Retrieved from http://www.uazone.org/demch/papers /cloudcom2012poster-bigdata-infra-v03.pdf

Dolan, K. M. (2004). Internet auction fraud: The silent victims. *Journal of Economic Crime Management*, *2*(1), 1-22.

Donald, I., Taylor, P., Johnson, S., Cooper, C., Cartwright, S., & Robertson, S. (2005). Work environments, stress, and productivity: An examination using ASSET. *International Journal of Stress Management*, *12*(4), 409.

Dukes, S. (1984). Phenomenological methodology in the human sciences. *Journal of Religion and Health*, *23*(3), 197-203.

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analyzing online social engineering attack surfaces. *Computers & Security*, *69*, 18-34.

Ekman, P. (1991). *Telling lies: Clues to deceit in the marketplace, politics, and marriage.* New York, NY: W.W. Norton.

Ekman, P. (1996). Why don't we catch liars? *Social Research*, 801-817.

Ekwall, D., & Rolandsson, B. (2013). Security aspects on corporate culture in a logistics terminal setting. *Journal of Transportation Security*, *6*(1), 13-25. doi:10.1007/s12198-012-0100-0

Evans, N. J. (2009). *Information technology social engineering: An academic definition and study of social engineering - analyzing the human firewall* (Order No. 3369832). Available from ProQuest Dissertations & Theses Global. (304906653). Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu/docview/304906653?accountid=12085

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

FBI Internet Complaint Center. (2018, October 12). "Common fraud schemes: Internet fraud." *FBI.gov.* Retrieved from https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud

Field, T. (2016). Email security. Social Engineering Report 2016. *Information Security Media Group.* Retrieved from https://www.agari.com/email-security/whitepapers/email-security-and-social-engineering-survey.pdf

FIPS PUB 199. (2004, February). Standards for Security Categorization of Federal Information and Information Systems. *FIPS*. Gaithersburg, MD: U.S. Department of Commerce. doi:10.1.1.8.5174&rep=rep1&type=pdf

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26-44.

Fu, J., & Chen, J. H. F. (2015). Career commitment of information technology professionals: The investment model perspective. *Information & Management*, *52*(5), 537-549. doi:10.1016/j.im.2015.03.005

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*(9), 1408-1416.

Gamble, J. E., Thompson, A. A., & Peteraf, M. A. (2013). *Essentials of strategic management: The quest for competitive advantage* (5th ed.). New York, NY: McGraw-Hill/Irwin.

Gardner, B., & Thomas, V. (2014). *Building an information security awareness program: Defending against social engineering and technical threats*. London, UK: Elsevier.

Godin, G., Bélanger-Gravel, A., Eccles, M., & Grimshaw, J. (2008). Healthcare professionals' intentions and behaviours: A systematic review of studies based on social cognitive theories. *Implementation Science*, *3*(1), 36.

Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. *Security Focus*, *December 18*.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of unintentional insider threats deriving from social engineering exploits. Paper presented at the 236-250. Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu/docview/1687235742?accountid=12085

Haber, L. (2009). Security training 101. *Network World*, *26*(16), 30-33.

Hagel, J. (2014). Nine ways to improve data security. *Journal of Accountancy*, *218*(3), 22-23.

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. doi:10.1016/j.chb.2016.03.026

Hasan, M., Prajapati, N., & Vohara, S. (2010). Case study on social engineering techniques for persuasion. *arXiv preprint arXiv:1006.3848*.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, *100*(4), 817-885.

Hawkins, N. (2017). Why communication is vital during a cyber-attack. *Network Security*, *2017*(3), 12-14. doi:10.1016/S1353-4858(17)30028-4

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a Decision-Theoretic approach. *Risk Analysis*, *38*(2), 215-225. doi:10.1111/risa.12878

Hinson, G. (2008). Social engineering techniques, risks, and controls. *EDPAC: The EDP Audit, Control, and Security Newsletter*, *37*(4-5), 32-46.

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber-attack business: A survey. *ACM Computing Surveys (CSUR)*, *51*(4), 1-36. doi:10.1145/3199674

Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009, August). Towards automating social engineering using social networking sites. In *Computational Science and Engineering, 2009. CSE'09. International Conference on* (Vol. 3, pp. 117-124). IEEE.

IBM. (2016). The 2016 IBM Cybersecurity Intelligence Index. *IBM Security Services.* Retrieved from https://www.slideshare.net/KanishkaRamyar/the-ibm-x-force-2016-cyber-security-intelligence-index

IBM. (2017). The IBM X-Force Threat Intelligence Index 2017. *IBM X-Force.* Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwjdzILKyuDeAhUJZawKHbOaDbIQFjABegQIBRAC&url=https%3A%2F%2Fwww.leadersinsecurity.org%2Fcomponent%2Fphocadownload%2Fcategory%2F11-2017-cybersecurity-publications.html%3Fdownload%3D185%3A2017-cybersecurity-publications&usg=AOvVaw2-CFZ-a4WrLSZ2e-lBCqli

IDG. (2015, October). 2016 Global state of information security survey. *Tech Research.* Retrieved from https://www.idg.com/tools-for-marketers/2016-global-state-of-information-security-survey/

Ilves, T. H. (2016). The consequences of cyber-attacks. *Journal of International Affairs*, *70*(1), 175-181.

Indrajit, R. E. (2017). Social engineering framework: Understanding the deception approach to human element of security. *International Journal of Computer Science Issues*, *14*(2), 8-16. doi:10.20943/01201702.816

Information Systems Audit and Control Association. (2016). State of cybersecurity implications for 2016: An ISACA and RSA conference survey. *Cybersecurity Nexus.* Retrieved from https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

Jackson, T. J. (2017). *Social engineering and enterprise security: An exploratory qualitative case study* (Order No. 10749719). Available from ProQuest Dissertations & Theses Global. (2029241574). Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu/docview/2029241574?accountid=12085

Jiang, J. J., Huang, W., Klein, G., & Tsai, J. C. (2018). The career satisfaction of IT professionals with mixed job demands. *IEEE Transactions on Engineering Management*, 1-12. doi:10.1109/TEM.2018.2870085

Johnson, J. V., & Hall, E. M. (1988). Job strain, work place social support, and cardiovascular disease: A cross-sectional study of a random sample of the Swedish working population. *American Journal of Public Health*, *78*(10), 1336-1342.

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, *66*, 75-87.

Kadivar, M. (2014). Cyber-attack attributes. *Technology Innovation Management Review*, *4*(11), 22-27. doi:10.22215/timreview/846

Karasek, R. A. (1979). Job demands, job decision latitude, and mental strain: Implications for job redesign. *Administrative Science Quarterly*, 285-308.

Karasek, R. A., & Theorell., T. (1990). Healthy work: Stress, productivity, and the reconstruction of working life. *The American journal of Public Health*, *80*, 1013-1014.

Keller, T., & Alsdorf, K. L. (2012). *Every good endeavor: Connecting your work to God's work.* New York, NY: Dutton.

Kessler, W. A. (2016). *Effectiveness of the protection motivation theory on small business employee security risk behavior* (Order No. 10164688). Available from ProQuest Dissertations & Theses Global. (1896581541). Retrieved from http://ezproxy

.liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu/docview/1896581541?accountid=12085

Krathwohl, D. R. (2009). *Methods of educational and social science research: The logic of methods*. Long Grove, IL: Waveland Press.

Krunal, G., & Viral, P. (2017). Survey on ransomware: A new era of cyber-attack. *International Journal of Computer Applications*, *168*(3), 38-41. doi:10.5120/ijca2017914446

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy*, *4*(1), 33-39.

Lavion, D. (2018). Pulling fraud out of the shadows: Global economic crime and fraud 2018. *PwC.* Retrieved from https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf

LeRouge, C., Nelson, A., & Blanton, J. E. (2006). The impact of role stress fit and self-esteem on the job attitudes of IT professionals. *Information & Management*, *43*(8), 928-938. doi:10.1016/j.im.2006.08.011

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: Rand Corporation. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a508151.pdf

Lim, V. K., & Teo, T. S. (1999). Occupational stress and IT personnel in Singapore: Factorial dimensions and differential effects. *International Journal of Information Management*, *19*(4), 277-291.

Lincoln, Y. S., & Denzin, N. K. (Eds.). (1998). *The landscape of qualitative research: Theories and issues*. Thousand Oaks, CA: Sage.

Lineberry, S. (2007). The human element: The weakest link in information security. *Journal of Accountancy*, *204*(5), 44-46,49.

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. *Information Resources Management Journal (IRMJ)*, *24*(3), 1-8.

Maan, P. S., & Sharma, M. (2012). Social engineering: A partial technical attack. *International Journal of Computer Science Issues (IJCSI)*, *9*(2), 557-559.

Magnusson, E., & Marecek, J. (2015). *Doing interview-based qualitative research: A learner's guide*. Cambridge, UK: Cambridge University Press.

Manadhata, P. K., & Wing, J. M. (2010). An attack surface metric. *IEEE Transactions on Software Engineering*, *37*(3), 371-386.

Mann, I. (2017). *Hacking the human: Social engineering techniques and security countermeasures*. Oxfordshire, UK: Routledge.

Manske, K. (2000). An introduction to social engineering. *Information Systems Security*, *9*(5), 1-7.

Mckoy, C. (2015). *Social engineering attacks on organizations in the 21st century* (Order No. 1587692). Available from ProQuest Dissertations & Theses Global. (1681623489). Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu/docview/1681623489?accountid=12085

Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the vulnerability of US hospitals to social engineering attacks: How many of your employees would share their password? *International Journal of Information Security and Privacy (IJISP)*, *2*(3), 71-83.

Messersmith, J. (2007). Managing work-life conflict among information technology workers. *Human Resource Management: Published in Cooperation with the School of Business Administration, The University of Michigan and in alliance with the Society of*

Human Resources Management, *46*(3), 429-451.

Mills, D. (2009). Analysis of a social engineering threat to information security exacerbated by vulnerabilities exposed through the inherent nature of social networking websites. *Proceedings of the 2009 Information Security Curriculum Development Annual Conference*, *InfoSecCD'09* (2009), 139-141. Association for Computing Machinery

Mishra, D., Akman, I., & Mishra, A. (2014). Theory of reasoned action application for green information technology acceptance. *Computers in Human Behavior*, *36*, 29-40.

Moen, P., Kelly, E. L., Fan, W., Lee, S., Almeida, D., Kossek, E. E., & Buxton, O. M. (2016). Does a flexibility/support organizational initiative improve high-tech employees' well-being? Evidence from the work, family, and health network. *American Sociological Review*, *81*(1), 134-164. doi:10.1177/0003122415622391

Moore, J. E. (2000). One road to turnover: An examination of work exhaustion in technology professionals. *MIS Quarterly*, *24*(1), 141.

Mourmant, G., Gallivan, M. J., & Kalika, M. (2009). Another road to IT turnover: The entrepreneurial path. *European Journal of Information Systems*, *18*(5), 498-521. doi:10.1057/ejis.2009.37

Moustakas, C. E. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186-209. doi:10.1016/j.cose.2016.03.004

Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. *Computers & Security*, *55*, 114.

Nagy, K., Hale, B., & Strouble, D. (2010). Verify then trust: A new perspective on preventing social engineering. Paper presented at the 259-XIII. Retrieved from http://ezproxy .liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu /docview/869617328?accountid=12085

National Institute of Standards and Technology (NIST). (1998, April). *Information technology training requirements: A role- and performance-based model* (NIST Special Publication 800-16). Washington, D.C.: U.S. Department of Commerce. Retrieved from https: //nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

National Research Council. (2009). *Technology, policy, law, and ethics regarding US acquisition and use of cyber-attack capabilities*. Washington, DC: National Academies Press.

Nohlberg, M. (2008). *Securing information assets: Understanding, measuring and protecting against social engineering attacks* (Doctoral dissertation, Institutionen för data-och systemvetenskap (tills m KTH).

O'Dowd, A. (2017). Major global cyber-attack hits NHS and delays treatment. *Bmj*, *357*, j2357. doi:10.1136/bmj.j2357

O'Halloran, C., Robinson, T. G., & Brock, N. (2017). Verifying cyber-attack properties. *Science of Computer Programming*, *148*, 3-25. doi:10.1016/j.scico.2017.06.006

Ongori, H., & Agolla, J. E. (2008). Occupational stress in organizations and its effects on organizational performance. *Journal of Management Research*, *8*(3), 123.

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). *The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In* Proceedings of the 5th conference on Information technology education (pp. 177-181). ACM. doi:10.1145/1029533.1029577

Padilla, R. (2003). Clara: A phenomenology of disability. *American Journal of Occupational Therapy*, *57*(4), 413-423.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2015). *Human Factors and Information Security: Individual, Culture and Security Environment, Report published by Defence Science and Technology Organisation*. DSTO-TR-2484, Edinburgh South Australia, Australia. Retrieved from https://pdfs.semanticscholar.org /07f8/c87e6bb79ffb3ad846168a641dc750cb85e8.pdf

Peltier, T. R. (2006). Social engineering concepts and solutions. *Edpacs*, *33*(8), 1-13.

Pinnegar, S., & Daynes, J. G. (2007). Locating narrative inquiry historically. *Handbook of narrative inquiry: Mapping a Methodology*, 3-34.

Pipkin, D. L. (2003). *Halting the hacker: A practical guide to computer security* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Polkinghorne, D. E. (1989). Phenomenological research methods. In *Existential-phenomenological perspectives in psychology* (pp. 41-60). Springer, Boston, MA.

Ponemon Institute. (2017). *Cost of Cyber Crime Study, Ponemon Institute LLC*. Ponemon Institute Research Report. Traverse City, MI: Ponemon Institute in Collaboration with HP.

Ponemon Institute. (2017b, September). Keeper Security 2017 state of cybersecurity in small & medium-sized businesses (SMB). *Ponemon Institute*. Retrieved from https: //keepersecurity.com/assets/pdf/Keeper-2017-Ponemon-Report.pdf

Positive Technologies. (2018). How the human factor puts your organization at risk. *PtSecurity.com*. Retrieved from https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Social-engineering-2018-eng.pdf

Price, J. H., & Murnan, J. (2004). Research limitations and the necessity of reporting them. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/19325037.2004.10603611

Proof Point. (2018). The human factor 2018: People-centered threats define the landscape. *Proofpoint.com.* Retrieved from https://www.proofpoint.com/sites/default/files/pfpt-uk-tr-the-human-factor-2018.pdf

Rajeswari, K. S., & Anantharaman, R. N. (2005). Role of human-computer interaction factors as moderators of occupat*ional stress and work exhaustion. International Journal of Human-Computer Interaction*, *19*(1), 137-154. doi:10.1207/s15327590ijhc1901_9

Rana, M. M., Li, L., & Su, S. W. (2018). Cyber-attack protection and control of microgrids. *IEEE/CAA Journal of Automatica Sinica*, *5*(2), 602-609. doi:10.1109/JAS.2017.7510655

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector* (No. CMU/SEI-2004-TR-021). Carnegie-Mellon Univ.: Pittsburgh, PA Software Engineering Inst.

Rasmussen, J. (1982). Human errors. A taxonomy for describing human malfunction in industrial installations. *Journal of Occupational Accidents*, *4*(2-4), 311-333.

Reagin, M. J., & Gentry, M. V., F.A.C.H.E. (2018). Enterprise cybersecurity: Building a successful defense program. *Frontiers of Health Services Management*, *35*(1), 13-22. doi:10.1097/HAP.0000000000000037

Rege, A. (2016, June). Incorporating the human element in anticipatory and dynamic cyber defense. In *Cybercrime and Computer Forensic (ICCCF), IEEE International Conference on* (pp. 1-7). IEEE.

Rege, A., Adams, J., Parker, E., Singer, B., Masceri, N., & Pandit, R. (2017). Using cyber-security exercises to study adversarial intrusion chains, decision-making, and group dynamics. *European Conference on Cyber Warfare and Security*, 351-360.

Rößling, G., & Müller, M. (2009). Social engineering: A serious underestimated problem. *SIGCSE Bulletin*, *41*(3), 384.

Rocha Flores, W., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security*, *22*(4), 393-406.

Rotvold, G. M. (2007). *Status of security awareness in business organizations and colleges of business: An analysis of training and education, policies, and social engineering testing* (pp. 1-130). The University of North Dakota.

Rotvold, G. M. (2008). How to create a security culture in your organization. *Information Management Journal*, *42*(6), 32-34,36-38.

Salanova, M., Peiró, J. M., & Schaufeli, W. B. (2002). Self-efficacy specificity and burnout among information technology workers: An extension of the job demand-control model. *European Journal of Work and Organizational Psychology*, *11*(1), 1-25.

Sandberg, J. (2000). Understanding human competence at work: An interpretative approach. *Academy of Management Journal*, *43*(1), 9-25.

Schaab, P., Beckers, K., & Pape, S. (2017). Social engineering defense mechanisms and counteracting training strategies. *Information and Computer Security*, *25*(2), 206-222. doi:10.1108/ICS-04-2017-0022

Semer, L. J. (2012). Evaluating the employee security awareness program: regular audits of IT safeguards can reveal whether staff members are doing their part to protect the organization's data and networks. *Internal Auditor*, *69*(6), 53-57.

Shih, S., Jiang, J. J., Klein, G., & Wang, E. (2013). Job burnout of the information technology worker: Work exhaustion, depersonalization, and personal accomplishment. *Information & Management*, *50*(7), 582-589. doi:10.1016/j.im.2013.08.003

Shoniregun, C. A., Dube, K., & Mtenzi, F. (2010). Introduction to E-Healthcare Information Security. In *Electronic Healthcare Information Security* (pp. 1-27). Springer, Boston, MA.

Simon, M. K., & Goes, J. (2013). *Excerpt from* (Dissertation and scholarly research: Recipes for success). College Grove, OR: Dissertation Success, LLC. Retrieved from http: //www.dissertationrecipes.com/wp-content/uploads/2011/04/Assumptions -Limitations-Delimitations-and-Scope-of-the-Study.pdf

Slevin, E., & Sines, D. (1999). Enhancing the truthfulness, consistency and transferability of a qualitative study: Utilizing a manifold of approaches. *Nurse Researcher (through 2013)*, *7*(2), 79.

Spinapolice, M. (2011). *Mitigating the risk of social engineering attacks* (Order No. 1503083). Available from ProQuest Dissertations & Theses Global. (913498347). Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com.ezproxy .liberty.edu/docview/913498347?accountid=12085

Stake, R. E. (2010). *Qualitative research: Studying how things work*. New York, NY: Guilford Press.

Stewart Jr, J. H. (2015). *Social engineering deception susceptibility: Modification of personality traits susceptible to social engineering manipulation to acquire information through attack and exploitation* (Order No. 3717295). Available from ProQuest Dissertations & Theses Global. (1711739305). Retrieved from http: //ezproxy.liberty.edu/login ?url=https://search-proquest-com .ezproxy.liberty .edu/docview/1711739305?accountid =12085

Strauss, A., & Corbin, J. M. (1997). *Grounded theory in practice*. Thousand Oaks, CA: Sage.

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, *68*(3), 226.

Symantec. (2017, April). Internet security threat report. *Symantec.com.* Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Tarallo, H. M. (2015). *Social engineering—countermeasures and controls to mitigate hacking* (Order No. 1588867). Available from ProQuest Dissertations & Theses Global. (1689458229). Retrieved from http://ezproxy.liberty.edu/login?url=https: //search-proquest-com.ezproxy.liberty.edu/docview/1689458229 ?accountid=12085

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, *32*(10), 1014-1023. doi:10.1080/0144929X.2013.763860

Thornburgh, T. (2004, October). Social engineering: The dark art. In *Proceedings of the 1st Annual Conference on Information Security Curriculum Development* (pp. 133-135). ACM.

Torten, R. J. (2018). *A quantitative regression study of the impact of security awareness on information technology professionals' desktop security behavior* (Order No. 10681492). Available from ProQuest Dissertations & Theses Global. (1973192341). Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu/docview/1973192341?accountid=12085

Torten, R. J., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security*, *79*, 68-79. doi:10.1016/j.cose.2018.08.007

U.S. Department of Labor, Bureau of Labor Statistics. (2018). Computer and information technology occupations. *Occupational outlook handbook.* Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/home.htm

U.S. Department of Labor, Bureau of Labor Statistics. (2018b). Information security analysts. *Occupational outlook handbook.* Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/home.htm

Van Manen, M. (2016a). *Phenomenology of practice: Meaning-giving methods in phenomenological research and writing*. Abingdon, Oxon, UK: Routledge.

Van Manen, M. (2016b). *Researching lived experience: Human science for an action sensitive pedagogy* (2nd ed.). Abingdon, Oxon, UK: Routledge.

Verizon. (2013). 2013 Data breach investigations report (11th ed.). *Verizon.* Retrieved from https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

Verizon. (2018). 2018 Data breach investigations report: Executive summary (11th ed.). *Verizon.* Retrieved from https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

Verizon. (2018b). 2018 Data breach investigations report (11th ed.). *Verizon.* Retrieved from https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

Viljoen, J. P., & Rothmann, S. (2009). Occupational stress, ill health and organizational commitment of employees at a university of technology. *SA Journal of Industrial Psychology*, *35*(1), 67-77.

Walko, E. S. (2013). *Social engineering exploits in the private business sector: Identifying the problem and designing a defense* (Order No. 1550017). Available from ProQuest Dissertations & Theses Global. (1491381103). Retrieved from http://ezproxy.liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu/docview/1491381103?accountid=12085

Weigl, M., Stab, N., Herms, I., Angerer, P., Hacker, W., & Glaser, J. (2016). The associations of supervisor support and work overload with burnout and depression: A cross-sectional study in two nursing settings. *Journal of Advanced Nursing*, *72*(8), 1774-1788.

Wolgemuth, J. R., Hicks, T., & Agosto, V. (2017). Unpacking assumptions in research synthesis: A critical construct synthesis approach. *Educational Researcher*, *46*(3), 131-139. doi:10.3102/0013189X17703946

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, *16*(6), 315-331.

Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security*, *16*(5), 463-483. doi:10.1108/09685220810920549

Workman, M. (2008b). 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.

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage.

Zhan, Z., Xu, M., & Xu, S. (2015). Predicting cyber-attack rates with extreme values. *IEEE Transactions on Information Forensics and Security*, *10*(8), 1666-1677. doi:10.1109/TIFS.2015.2422261

Zheng, K., Wu, T., Wang, X., Wu, B., & Wu, C. (2019). A session and dialogue-based social engineering framework. *IEEE Access*, *7*, 67781-67794. doi:10.1109/ACCESS.2019.2919150

Appendix A: Interview Script

Hello, thank you for taking the time to meet with me today. As you may recall, I am Lily Pharris, a doctoral student in the School of Business at Liberty University, and I am conducting research as part of the requirements for a Doctor of Business Administration degree. The purpose of my research is to investigate how IS professionals make sense of their lives and experiences as they deal with social engineering attacks at their company.

[Hand Participant Copy of Previously Signed/Submitted Informed Consent]

Before we begin, I want to remind you that participation in this study is voluntary, and your decision to participate will not affect your current or future relationship with Liberty University. If you decide to participate, you are free not to answer any question or withdraw at any time without affecting those relationships.

Additionally, I want to make sure you know that the records of this study will be kept confidential. Data and recordings will be stored securely on a password protected zip drive for three years following the study, and only I will have access to retrieve those files. In any sort of report I might publish, I will not include any information that will make it possible to identify you or your employer. While it is possible that I may share the data I collect from you with other researchers or in other studies, if I share anything, I will remove any information that could identify you or your employer before sharing. After three years, all electronic records will be deleted.

You have already reviewed, signed, and submitted the informed consent policy. At this point, do you have any questions you would like to ask me before we begin the interview?

Again, thank you for agreeing to participate in this interview today. As we begin, please take a moment to focus on your experiences as an IS professional as they relate to preventing social engineering vulnerabilities at your workplace.

1. Try to remember one of the last times you had to deal with a social engineering vulnerability at your work. Tell me about the situation, including how you felt and responded. Who was involved and what was said as you were addressing the situation?
    a. What was going on or what were you doing just before you learned about a social engineering attack or vulnerability at your workplace?
    b. How did the experience affect you? What changes do you associate with the experience?
    c. What feelings do you recall were generated when you realized a social engineering vulnerability had been exploited?
    d. What thoughts stand out in your memory as you attempted to address or prevent the vulnerability?
    e. Were you aware of any physical reactions or changes in your state of mind at the time?
    f. What other elements, incidents, and people closely connected to the experience stand out to you from this experience?
    g. Besides preventing social engineering vulnerabilities, what other job functions and duties are you responsible for at your place of employment?
    h. When considering all the activities you engage in, including addressing social engineering vulnerabilities, how does everything get accomplished?

   i. What resources do you have at your disposal to prevent social engineering across your organization?
   j. How adequate are these resources to accomplish the task of preventing, if not eliminating, social engineering attacks on your organization?
   k. Have you shared all that is significant with reference to this personal experience of preventing social engineering vulnerabilities at your workplace?

2. Social engineering attacks typically target and exploit the people of an organization—preying on a person's natural curiosities or inclination to trust and help others. Other times social engineers use fear or pressure to compel people to respond. To what extent do you believe the vulnerabilities related to the "human element" can be eliminated?
   a. How does this belief influence how you address social engineering attacks at your organization?
   b. What risks do social engineering attacks pose to your company?
   c. How is the responsibility of addressing and preventing social engineering vulnerabilities at your company designated or assigned at your organization? Single individual? IS team? Everyone?
   d. How much time and effort do you (or your team/department) devote to the prevention of social engineering vulnerabilities at your organization?
   e. Given your current level of resources (including manpower, training, budget, etc.) and your understanding of the level of risk social engineering attacks pose toward your organization, please describe the extent you believe the amount of time and effort devoted toward preventing social engineering across your organization is appropriate.

3. What conditions, situational or environmental, have influenced, or are currently influencing, how your organization has chosen to address security vulnerabilities related to human manipulation, as is often targeted in social engineering attacks?
4. Describe what steps or improvements, if any, you (inclusive of the IS team and organization) have taken to move the company from being vulnerable to social engineering attacks to protected against social engineering attacks.
    a. Please explain to what extent you are pleased with this transformation.
    b. Please explain to what extent you believe more needs to be done.
    c. Please explain to what extent you believe more will be done to improve your defenses against social engineering attacks.
5. Are you aware of any tactics that have been used to successfully reduce social engineering attacks in other businesses or industries? Please describe an example that comes to mind.
    a. To what extent do you believe tactics that have been successful in other industries are applicable in your current industry? Why or why not?
    b. What differences do you believe exist between your industry and those industries that make them more or less successful than you have experienced at your organization?
6. What meaning, if any, do you ascribe to the work you do to prevent social engineering vulnerabilities at your company?
    a. How does the work that you do to address social engineering attacks at your organization impact your company?

b. To what extent would you consider the work that you do to prevent social engineering vulnerabilities as meaningful? Why?

c. To what extent do social engineering attacks on your organization bother you? Why?

7. Have you shared all that is significant with reference to your personal experiences preventing social engineering vulnerabilities at your workplace?
8. For my final question, would you be willing to recommend another IS professional from the region who works in your company or industry who has experiences with preventing social engineering vulnerabilities as part of their professional job duties?

I truly appreciate you taking the time to meet with me and answer these questions today. My next step is to transcribe the interview, and once the transcription is complete, I will share a copy with you to review and check for accuracy. You will have the opportunity at that time to address any points you feel are unclear or could benefit from additional clarification. If you think of anything else that should be considered, feel free to call me at 318-229-3643, or email me at [redacted]. Do you have any questions, comments, or concerns at this time?

Thanks again for helping me with my study.