Interpersonal dimensions of information security

by

Alexandra Pimentel

B.A., University of Dallas, 2013
M.A., Kansas State University, 2016

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Sociology, Anthropology, and Social Work
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2022

Abstract

This dissertation is a qualitative examination of three dimensions related to the phenomenon of social engineering. The first analysis examines the affective experience of engaging in social engineering perpetration. The results of this analysis detail the range and intensity of emotions experienced by social engineers through the course of a social engineering attempt, as well as the way in which the affective experience is mediated through interactions with targets and understandings of self. The second analysis examines how social engineers maintain deceptions across a social engineering attempt. This analysis found that social engineers employ two distinct forms of deception, bluff and stealth, and elucidates how social and technological factors are utilized by social engineers to maintain both these types of deception. The last analysis turns to the targets of social engineering, and examines how these targets engage in deception detection, which may prevent social engineering attempts from being successful. The results of this analysis find that deception detection is characterized as the target being able to detect anomalies in communications and interactions with social engineer. The results explicate the perceptual and cognitive aspects of deception detection, as well as highlight the role of knowledgeable entities, rather than individuals alone, in the accomplishment of deception detection.

Interpersonal dimensions of information security

by

Alexandra Pimentel

B.A., University of Dallas, 2013
M.A., Kansas State University, 2016

A DISSERTATION

submitted in partial fulfillment of the requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Sociology, Anthropology, and Social Work
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2022

Approved by:

Major Professor
Dr. Kevin Steinmetz

Copyright

Abstract

This dissertation is a qualitative examination of three dimensions related to the phenomenon of social engineering. The first analysis examines the affective experience of engaging in social engineering perpetration. The results of this analysis detail the range and intensity of emotions experienced by social engineers through the course of a social engineering attempt, as well as the way in which the affective experience is mediated through interactions with targets and understandings of self. The second analysis examines how social engineers maintain deceptions across a social engineering attempt. This analysis found that social engineers employ two distinct forms of deception, bluff and stealth, and elucidates how social and technological factors are utilized by social engineers to maintain both these types of deception. The last analysis turns to the targets of social engineering, and examines how these targets engage in deception detection, which may prevent social engineering attempts from being successful. The results of this analysis find that deception detection is characterized as the target being able to detect anomalies in communications and interactions with social engineer. The results explicate the perceptual and cognitive aspects of deception detection, as well as highlight the role of knowledgeable entities, rather than individuals alone, in the accomplishment of deception detection.

Table of Contents

Acknowledgements

I would first like to thank my entire committee for sticking with me for years through a global pandemic while I struggled to turn a proposal into a dissertation. Ya'll are the best.

A huge thank you to Dr. Kevin Steinmetz: I owe you a debt of gratitude that extends far beyond this dissertation. Your mentorship has improved my life as both a scholar and as a professional. There is a long roster of evidence to support this claim that I could list here, but this dissertation is already long enough. Thank you for the little things, like helping me become passable at public speaking, and the bigger things, like introducing me to this world of social engineering, security auditors, and cybersecurity.

Thank you also to Dr. Lisa Melander. Your mentorship and guidance in my M.A. program gave me the confidence and skills that I needed to continue on to a doctoral program. I appreciate your continued support and role on my dissertation committee. Dr. Gerad Middendorf, thank you for your support on my committee, and also for my introduction to many of the ideas within sociology, which I first became acquainted with while taking your Contemporary Sociological Theory class (back in 2015!). Some of those ideas have made their way into this dissertation. My appreciation and thanks also to Dr. Eugene Vasserman for the cybersecurity expertise that you bring to the committee and your willingness to cross over the theoretical divide between the disciplines of sociology and computer science. Lastly, thank you to all the Kansas State University graduate students who I met and became friends with during my time here. I will always remember your support and kindness during long days and late nights.

Chapter 1 - Introduction

In the context of information security, the term social engineering is used to encompass a broad range of deceptive interactions. Though definitions vary, social engineering can generally be understood as the deception and manipulation of individuals for the purposes of circumventing information security measures. Social engineers may target sensitive or personal information, often with the objective of gaining access to a system to steal data or money. For organizations, these deceptions can be costly. In one example, MacEwan University lost $11.8 million in 2017 from an online phishing scam (CBC, 2018). In this social engineering attack, university staff members were convinced through email messages to change over the banking information of a legitimate vendor to scammer-operated overseas bank accounts. In 2019, an even larger sum of money was lost by a subsidiary of Toyota, when the company suffered a $37 million dollar loss from a business email compromise (BEC) scam in which attackers convinced employees to change account information that allowed funds to be electronically transferred to the scammers (Forbes, 2019). In 2021, the FBI's Internet Crime Complaint Center reported receiving complaints from around 20,000 organizations which collectively had lost over 2.4 billion dollars to such BEC attacks (IC3, 2021).

Individuals may also be subjected to social engineering exploitation. For instance, social engineering techniques may be used in romance frauds, a kind of scam where a target is made to believe they are in an intimate relationship with the fraudster who abuses this perception to ply money from the victim's hands (Cross, 2015; 2016). Although romance frauds have been occurring for decades, a recent example of romance fraud perpetration received extensive coverage, including in Netflix's (2022) documentary *The Tinder Swindler*. This documentary investigated Shimon Hayut, a social engineer with multiple convictions for fraud, who purportedly defrauded multiple women who he met on a dating app of millions of dollars through romance scams (Netflix, 2022).

While the social engineering attacks discussed thus far are particularly high-profile examples, these incidents are part of the persistent barrage of social engineering attempts that have become a feature of modern life for many. Citizens of the United States have lost millions of dollars in social engineering scams that occur over email, phone calls, or in-person from social engineers who purport to be from the IRS and claim to be collecting unpaid taxes or who fraudulently convince people to reveal their social security numbers (IRS, 2019). Verizon (2018) reports that 96 percent of social engineering attacks reported by organizations for the year occurred over email. The report notes that while only an estimated 4 percent of users were duped by any one phishing campaign, those same users were likely to repeatedly fall for such scams (Verizon, 2018). A 2021 Verizon report also reported phishing was a factor in up to 36% of breaches in which data was disclosed.

The magnitude of social engineering attempts has galvanized organizations and businesses into action over the past two decades. Some of the impetus to contend against social engineering emerges from the development of cybersecurity control recommendations for the private sector, which began with the enactment of laws like the Federal Information Security Modernization Act (2002) and curation of security standards such as the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (2014). Economic factors have also contributed to the rise of systematic attention paid to cybersecurity and social engineering by organizations. One estimate of this economic impact is that the average dollar cost of a single security breach is 3.86 million, according to an IBM sponsored study conducted by the Ponemon Institute (2018).

Adaptations by organizations to bolster information security and to contend against social engineering tend to focus on the implementation of technological security controls as well as security awareness policies and trainings. This orientation towards mitigating social engineering risk tends to lack an understanding of the intrinsic role of social interaction in the perpetration and detection of social engineering. McGuire (2018) frames this lack of consideration as an issue plaguing the conceptualization of cybercrime in general. He states that research in this area has failed to recognize "…that problems rooted in social interaction are ultimately problems of social interaction rather than how those interactions are mediated" (McGuire, 2018, p. 137).

This dissertation agrees with McGuire's contention that issues of social interaction require social interaction itself to be given primacy as the focus of study. Contextualizing social engineering and security awareness as social interactions, rather than simply as concerns for information security programs, allows for a more holistic understanding of these concepts. A social engineering security breach is a manifestation of deception, which entails the exploitation of both individual credulity and the basic trust that underpins everyday interactions in society. Understanding interactional dynamics within social engineering and in this manner broadens the scope of analysis of these issues. Taking this orientation is crucial for advancing efforts to reduce social engineering susceptibility and increase resistance to social engineering, as social engineers rely on these dimensions of social interaction, even as their specific methods of deception change across time.

To examine the interactional dimensions and social context of social engineering and security awareness, this dissertation incorporates theoretical perspectives on interaction from sociological and criminological developments of symbolic interactionism, in addition to the interdisciplinary work on the theoretical dimensions of trust and deception, to explore resistance to social engineering, the interactional elements of social engineering perpetration, and elucidate the connection between these interactional dimensions and security awareness. Specifically, this dissertation examines the following research questions:

1. What are the experiential dimensions of engaging in social engineering? [1]
2. How do social engineers attempt to maintain deceptions while engaging in social engineering?
3. How does deception detection occur in social engineering interactions?

These research questions are examined through the analysis of qualitative data in the forms of individual semi-structured interviews conducted with social engineers and information security professionals as part of a National Science Foundation-funded research project [grant number SES-1616804] which ran from 2016-2019. Fifty-four participants were recruited for this qualitative project through snowball sampling, which is a standard recruitment process for qualitative research with participants with specialized knowledge in the research area of interest (Berg & Lune, 2012, Lindlof & Taylor, 2019). Three interview protocols were developed, which were tailored to the knowledge and experiences possessed by social engineers, security auditors, and information security professionals. The semi-structured interviews were confidentially conducted, recorded, and securely stored, and each participant was assigned as pseudonym. The interviews were then transcribed and de-identified.

Each of the research questions was analyzed through a grounded theory analytical approach, which provided structure to the process of analysis (Glaser & Strauss, 1967). The first research question, which examined the experience of social engineering, was analyzed using a

[1] The discussion and analysis of this research question draws extensively from an analysis that was subsequently published (see: Pimentel, A. & Steinmetz, K.F. (2021). Enacting social engineering: the emotional experience of information security deception. *Crime, Law, & Social Change*. https://doi.org/10.1007/s10611-021-09993-8)

subset (N=37) of the participant interviews, as only participants who had personally engaged in social engineering could provide insight into this research question. The second and third research questions included all participant interviews and were analyzed to examine the occurrence of deception detection in social engineering interactions and the ways in which social engineers maintain social engineering deceptions.

The methods used to recruit the sample of participants, collect the interview data, and analyze the data for this dissertation are discussed in detail in Chapter 3. Prior to discussing the research methods for this dissertation, there is a review of relevant literature. This literature review focuses on research and relevant theoretical perspectives on social engineering, social engineering deceptions, the detection of those deceptions, and the implications for security awareness.

Chapter 2 - Literature Review

The purpose of this literature review is to examine both prior work and theoretical perspectives that provide context to each of the three research questions to be investigated by this dissertation. To this end, the review first examines the concept of social engineering and research on fraud perpetration. The review then turns to an examination of relevant theoretical work. Specifically, the review draws on theoretical insights from phenomenology, symbolic interactionism, and cultural criminology, as these perspectives allow insight into the interactional dimensions and societal context of social engineering. Next, the review focuses on the process by which social engineers maintain deceptions. Relevant literature on persuasion is discussed, as well as the role of technologically mediated forms of communication and social structures more broadly. Lastly, there is a review of the relevant work on deception detection, which links research on deception detection to the context of social engineering and examines psychological and cognitive factors which may influence the ability of individuals to detect social engineering deceptions.

Social Engineering

Establishing the phenomenon[2]

This literature review first examines the concept of social engineering, particularly the ways in which this phenomenon is characterized across disciplines. This examination of the concept of social engineering contextualizes the theoretical approach of this dissertation, which approaches social engineering through an interactional lens. Literature on social engineering is produced within the fields of information security, business, psychology, and criminology. Under the purview of these disciplines, social engineering is often framed as any attack vector that exploits human psychology to compromise a secure system, typically with the implicit assumption that the social engineer has monetary gain as the end goal of this activity. This perspective of social engineering is reflected clearly in Twitchell's (2009) definition of the concept as "the exploitation of psychological triggers and cognitive biases as a means to gain authorized access to information or information systems" (p. 229). Conceptualizing social engineering within this paradigm has led to examinations of the motley of methods and tactics employed by social engineers, as well as exhaustive rumination over the potential psychological dimensions that could be at play in social engineering.

Social engineering can take place across most means of communication utilized in the present day. Social engineering occurs in person (Brody, Brizzee, & Cano, 2012; Mouton,

[2] As Robert K. Merton (1987, p. 6) notes: "The manifest advisability of establishing the phenomenon before undertaking to explain it has long been recognized in principle if not always observed in practice."

Leenen, & Venter, 2016; Peltier, 2006), and in the use of technology such as email, email attachments, telephones, instant messaging, websites, and social media (Abraham & Chengalur-Smith, 2010; Applegate, 2009; Dhiman, Wajid, & Quraishi, 2017; Jain, et al., 2016; Power & Forte, 2006; Weir, Toolan, & Smeed, 2011). These domains may facilitate social engineering by being used in the preparation for social engineering or as a component of achieving the goals of the social engineer. For example, a social engineer may engage in open-source intelligence (OSINT) gathering in person by dumpster diving for useful information about a company, then scour social media for public information on employees, prior to attempting to use the discovered information in social engineering an employee over the phone (Edwards, Larson, Green, Rashid, & Baron, 2017; Long, 2008).

Many of the specific social engineering strategies that take place across these various communication mediums have been classified and described. Social engineering in person might take place by such means as tailgating, which entails following an authorized person into a secure location, shoulder surfing, or inconspicuously looking at and remembering private information being used by another person, and the aforementioned dumpster diving (Brody, et al., 2012; Long, 2008). Over electronic communication, typically email, phishing occurs when individuals receive messages that attempt to convince them to divulge confidential information or to install malicious software (Aleroud & Zhou, 2017; Applegate, 2009). Spear phishing, a variant of phishing, occurs when the message is targeted based on some information about the recipient (Jagatic, Johnson, Jakobsson, & Menczer, 2007; Tuttle, 2016). Similarly, vishing refers to social engineering attempts that take place over the phone, while SMiShing designates the same process over text messages (Dhiman, et al., 2017). These efforts of cataloging and analyzing the plethora of social engineering techniques may well continue *ad infinitum*, as "effective social engineering is flexible and open-ended" (Manske, 2000, p. 53) and bound only by the limitations inherent in human communication itself.

It has been noted that the features characterizing incidents portrayed as social engineering vary to such an extent that a single definition of this concept cannot be provided (Ivaturi & Janczewski, 2011; Mouton, Leenen, & Venter, 2016; Steinmetz, Pimentel, & Goe, 2019). Social engineering has been construed by some as referring to situations in which employees are manipulated into compromising organizational security for malicious purposes (Krombholz, Hobel, Huber & Weippl, 2015; Tuttle, 2016). For others, social engineering does not necessarily entail malicious intent, but does denote the use of social methods to gain unauthorized access to information or systems (Hancock,1995; Mouton, Malan, Kimppa, & Venter, 2015). Yet others define social engineering even more broadly, as exemplified by the statement by Berti and Rogers (2002) that "…Social engineering is somewhat synonymous with conning or deceiving someone" (p. 52). The boundaries of activities and behaviors that constitute social engineering are not well-delineated, and actions that comprise social engineering may occur over a diverse range of contexts and be enacted to achieve a wide variety of ends.

Regardless of the conceptual ambiguity that surrounds social engineering, there is a common thread that runs through discussions and definitions of social engineering: Social engineering is, at its core, *social*. There is, therefore, an intrinsic interactional component of this phenomenon. As elucidated in the following section, the social dimension of social engineering frauds may resemble the interactional attributes of fraud more broadly.

Experiences of fraud perpetration

The first analysis involved in this dissertation concerns the emotional experiences involved in social engineering perpetration. Therefore, a review of scholarship on fraud perpetration experiences is necessary. Examinations of the experiences of professional thieves, con-artists, and other perpetrators of fraud have a long-standing presence in criminological research. Sutherland (1937/1989) suggests in his foundational work, *A Professional Thief,* that the activity of professional thieving is stressful, lacking in thrills, and is hard work (Sutherland, 1937/1989, pp. 141-142). As he explains, "writers of detective stories who have never stolen a quarter and have never been deprived of their liberty for an hour are the only ones who can perceive any clamor or pleasure in grifting" (Sutherland, 1937/1989, p. 141). Yet, Sutherland (1937/1989) also acknowledges in a footnote that contradicting evidence exists from a variety of sources, which suggests that there can be a thrill behind professional thievery.

In his seminal work *The Big Con,* Maurer (1940/1999) explores confidence games in the early 1900s and provides additional evidence that the sensual elements of defrauding are a vital component of the criminal experience as well as a significant motivator for his participants. Paralleling Sutherland, Maurer (1940/1999) acknowledges that such work can be less-than-glamourous and that fraudsters must fend off boredom. However, he also recognizes that grifting can be intensely stimulating. He writes:

> There is a thrill about big-con work which no other branch of the grift can duplicate. The confidence man extends himself fully while he works; all his faculties and abilities are called into play…each mark is a new challenge to his ingenuity; and, perhaps, most importantly, the stakes for which he plays are very high. (Maurer, 1940/1999, p. 172)

Thus, while many in confidence rackets were involved for financial gain, Maurer makes it clear it is impossible to discount the role of emotions in such crimes.

These findings are reflected in studies of the experiences of perpetrators of frauds that exploit telecommunications and other technological developments (Doocy, Shichor, Sechrest, &

Geis, 2008; Jackson, 1994; Shover, Coffey & Hobbs, 2003). For instance, Doocy et al. (2008) report a telemarketing fraudster saying, “I like to win. I like to win in all the games I play, you know. And the money is a reason to be there…But winning is what I want to do….I want to beat that person I am talking to on the phone” (p. 349). In other words, there is a game-like quality to such frauds which creates feelings of excitement and satisfaction (Williams & Milton, 2015, p. 43). For this reason, Williams and Milton (2015, p. 237) conclude that “conning is as addictive to a con artist as skydiving is to a thrill seeker.” In addition, these studies note that these forms of fraud often depend on the offender possessing interpersonal and communicative skills, as well as knowledge of how to exploit social or financial systems (Doocy, et al., 2008; Jackson, 1994; Shover, Coffey & Hobbs, 2003).

Shover, Coffey and Hobbs, (2003) argue that the technological transformations in work and social life that impact professionals everywhere have the same influence over perpetrators of telemarketing fraud, as “the telemarketing fraudster depends on networks of information that are largely indistinguishable from those that underpin the non-criminal sector” (p. 502). The use of communications technology may also change the emotional experience of perpetrating fraud, as Doocy, et al. (2008) elaborate in the findings of their study of telemarketing fraud that the scammers found it easier, both practically and emotionally, to manipulate victims over the phone than face-to-face.

While the research on fraud indicates that technological and societal transformations shape both the methods of fraud used and the experiences of the perpetrators of that fraud, the past decade has yielded scant academic research on the experiences of social engineering frauds or social engineers. Experiences of social engineering perpetration have, however, been discussed by practitioners of social engineering themselves. One such person is Kevin Mitnick, a phone phreaker, hacker, and social engineer who characterizes social engineering as a specialty "within the job classification of con artist" (Mitnick & Simon, 2003). Mitnick (2003) describes himself as driven by curiosity and enjoyment of the social engineering experience to exploit information from individuals, often through the use of psychological techniques such as building trust, producing sympathy, or leveraging intimidation. Security consultant Ian Mann (2008) similarly emphasizes psychological vulnerabilities to social engineering, and, in addition, argues that the communication medium through which social engineering occurs shapes the social engineer's approach, as face-to-face interactions require more skill than do technologically mediated ones. Chris Hadnagy (2011), another prominent social engineer, discusses how aspects of being a social engineer, such as communication techniques, building rapport, and confidence, allow for successful social engineering attempts.

The experiences of fraudsters and social engineers may be congruent along a variety of dimensions. While criminological literature has, in the past, analyzed the experiences of individuals engaged in a variety of frauds, relatively little investigation exists that analyzes the experiences of social engineer perpetrators. Concluding the discussion of past research on fraud and social engineering, this review now turns to a discussion of relevant theoretical perspectives on the dimensions of human experience in the interactional processes of social engineering frauds.

Experiencing social engineering: Theoretical approach

The theoretical approach described in this section was selected as it is appropriate for exploring the dynamic dimensions of social engineering interactions, in addition to elucidating the nuances of the affective experience of social engineering perpetration. Social engineering as a phenomenon tends to be examined from a fairly atheoretical perspective that results in a limited understanding of multidimensional factors that structure and influence this activity. Specifically, social engineering is often examined from the context of how static psychological characteristics of victims or tactics employed by social engineers may be influential in the success of social engineering (Applegate, 2009; Schaab, Beckers, & Pape, 2017). Phenomenological, interactionist, and cultural criminological theoretical perspectives provide insight into the dynamic interactional facets of social engineering and allow these interactional dimensions to be situated within a cultural milieu and historical context. These perspectives will be considered in the analysis of the research question: *What are the dimensions of the experience of social engineering?*

The use of these theoretical perspectives elucidates the foundational structure of social engineering: As distinctively structured social interaction between human beings, that occurs within a particular communication framework and cultural milieu. Analyzing social engineering as an interactional experience additionally highlights both the social engineer and the target as active subjects who reciprocally influence and are influenced by the other during a social engineering attempt. Here, drawing on the theoretical work of phenomenologists and symbolic interactionists becomes relevant to contextualizing the interactional experience of social engineering.

Phenomenology originated as a philosophical movement based on the thoughts of philosophers such as Husserl (1983/1913) and then was further developed by philosophers and social theorists. The overarching idea that shapes phenomenology is that nothing can be separated from one's consciousness of it (von Eckartsberg, 1998). Every experience is experienced by a unique individual who is located within a specific time and place and who has certain attitudes, plans, and concerns. This means that whenever a person sees or experiences something, they experience it through this unique perspective of their consciousness of whatever it is they are experiencing. In phenomenology, this perspective of the individual is referred to as intentionality (Churchill & Wertz, 2001). A central ontological stance taken by phenomenology is that humans constitute their worlds by intentionally and meaningfully attuning to their situated contexts (Churchill & Wertz, 2001; von Eckartsberg, 1998). Put more simply: human experience is human reality. The life-world then, emerges for a human being out of the interplay between the object revealed to consciousness, and the intentions, and therefore meanings, of that conscious experience of the object. Because the experience people have of their worlds is inexorably bound to their projects, goals, or intentions, all experience is meaningful and all experiences point back to the intentionality of the experiencing human. The relationship between meaning, intention, and experience entails that human action can then be understood as engaged in for some intentional (though not necessarily consciously known) purpose (Churchill & Wertz, 2001).

As intentionality is the mode by which humans encounter and constitute their life-world, it is also the mode by which humans encounter other humans. According to van den Berg (1972), "Interhuman relations manifest themselves as physiognomies of a world, as nearness or distance of duties or plans, of *objects*. Yet this answer cannot be complete. There is yet another contact between man and fellow man" (pp. 67-68). What is being emphasized here is that the encounter between one human and another is more than a mutual constituting of each as subjects or objects, but rather that there is something particular in the encountering of another human being. The centrality which phenomenology places on experience and meaning, including in interactional contexts, makes it the optimal perspective with which to examine the dimensions of the experience of social engineering.

From a phenomenological perspective, experience always occurs as a flow of feelings that bodily express the meanings by which individuals constitute their worlds (Gendlin, 1997). Emotional aspects of experience are therefore never simply a vestigial outcropping of experience but are instead expressions that delineate the significance of an experience. Investigating the emotions felt in experience is particularly revelatory of the implicit meanings that shape much of how people orient themselves and act in the world. The implicit nature of these understandings ought not imply that emotions are either less significant in the structure of an experience or that emotions are more difficult to analyze. Much of everyday experience is guided by implicit, yet strongly felt, understandings of the world, and these meanings are often clearly demonstrated by individuals without being explicitly symbolized. The emotional content of a situation is the primary manifestation of the meaning imbued within that instance for an individual (Gendlin, 1997). This connection between meaning and emotion is revealed by the colloquialism "to feel a certain way about a situation," indicating both an emotional state as well as an assertion about the significance of the incident (Gendlin, 1997).

As the experience of social engineering stems from social interaction, this study is also informed by symbolic interactionism which allows for consideration of two fundamental elements of social interaction: self and other(s). Symbolic interactionism is concerned with the process by which individuals interpret and apply meaning to the gestures and utterances of others, as well as the way in which individuals convey meaning to those others with whom they are interacting (Blumer, 1998). Blumer (1998), drawing on the work of George Herbert Mead, argues that the interpreting ability of individuals is a process of self-interaction which leads to action. This process of self-interaction shapes emotion, as emotions have a self-referential aspect, which reveals the meanings that individuals bring to bear on their conceptions of themselves (Glas, 2017). Self-interaction produces action when an individual "notes various things, defines and weighs them, projects out different possibilities of action, selects among them, makes decisions, and revises" (Blumer, 1998, p. 96). The emotional experience of social engineering may, in line with other forms of interaction, depend on some level of emotional management by the social engineer. This connection between self-reflection and emotion is also noted in Hochschild's (1983) work on emotion management, which notes that individuals compare their own emotional states to their perception of external emotional expectations, and then either engage in emotion work to bring their own emotions in alignment with the expectations or reject the expectations.

Contemplating the face-to-face social actions of individuals, Goffman (1956) suggests that every participant in an interaction acts to project a particular definition of the interactional situation to the other participants. For the other participants to accept the presented definition of reality, a coherent expression of reality must be presented that can be accepted as a valid definition of reality. The other participants may also use the performer's appearance and manner to evaluate what sort of person they are, and what role they are likely to take in the interaction. Further, symbolic interactionism also considers the role of emotions in social interaction. The other party in this performative interaction influences the emotional experience of the performer. Emotion management is relevant to the presentation of a definition of reality, as the performer must be able to have expressive control and conceal inappropriate emotions and display appropriate ones for the situation (Goffman, 1956, p. 138).

The other person in this performative interaction influences the emotional experience of the performer. Emotion management is relevant to the presentation of a definition of reality, as the performer must be able to have expressive control and conceal inappropriate emotions and display appropriate ones for the situation (Goffman, 1956, p. 138). Emotion is also an aspect related to the positive regard others have about the performer's presentation of reality and self—a concept Goffman (1967) calls face.

Face-work entails the actions taken by an individual to gain or save face. Gaining face is a positive affective experience, felt as pride or satisfaction. Losing face then is a negative emotional experience, in which a person feels embarrassed, ashamed, or flustered because the of the judgement of the other and loss of a valued aspect of self (Goffman, 1967). Notably, Goffman (1956) asserts that the others may destroy the face of a performer they catch telling blatant lies, because these others feel that the performer who tells such lies can never be considered trustworthy. If losing face is associated with an experience of unpleasant emotions, it follows that the experience of having face destroyed would be experienced as intensely negative. The emotional experience of social engineering may then be, to some degree, impacted by the social engineer's perception of their own face-work.

The meanings that individuals bring to the world are not created in a void, but emerge out of personal experiences, as well as the social structure in which a person is situated. The work of the cultural criminologists develops the connections between crime, emotion, and societal milieu by suggesting that felt experiences of the structure of modernity may invigorate individuals in the commission of actions that may be criminal. Lyng (1990) suggests that the bureaucratic economy of modernity fosters the experience of a life of constrained possibilities in which individuals feel forces outside of themselves determine their actions. A reaction to this loss of control over spontaneous human action, Lyng (1990) argues, is a form of voluntary risk-taking called edgework.

Edgework is a concept coined by Hunter S. Thompson (1967) in his work on the outlaw motorcycle gang Hell's Angels, which he used to refer to the experiential context of engaging in high-risk street racing. As noted by Thompson (1967), and subsequently developed by cultural criminologists (Ferrell, Hayward & Young, 2008), impulses to engage in edgework stem from the structure of late modern society in which "self-fulfillment, expression, and immediacy are paramount values, yet the possibilities of realizing such individualized dreams are strictly curtailed" (Ferrell, Hayward, & Young, 2008, p. 72). To establish meaning and identity in society, edgeworkers engage in risky activity that puts them dangerously near the edge of suffering the consequence of some danger and see themselves as relying on skill to prevent themselves from crossing over the edge of their activity into chaos and destruction. Engaging in edgework is experienced as exhilarating self-determination; a heightened sense of self and all of reality occurs and experiences of the passage of time changes.

Specifically focusing on criminal activities, Katz (1988) contends that the impetus to commit crime can lie in the constructions of the emotional experience of an illegal action. The choice to commit a crime, such as robbery, can lie in the thrill and excitement of the experience of committing the crime. The meaning of the criminal act is expressed in the emotions it provokes: a delight in causing chaos in an ordered system and thereby exerting control over the victim of the robbery (Katz, 1988).

Young (2003) develops and extends the premise of the emotional appeal in controlling the advent of chaos on self or others, by suggesting that the structure of late modernity results in both ontological and economic insecurities in which individuals lose their sense of identity and have a pervasive resentment towards an unstable and chaotic lived experience. Crime may then have the meaning of rebellion as a form of resistance against the social structure and be engaged in for the sake of transgressing societal rules or laws (Young, 2003). Ferrell (2004), in his analysis of modernity, further develops the connection between emotion, crime, and modernity by theorizing that excitement and human engagement, in both crimes and activities that cut against the routines and structures of modern life, disrupt normalcy and, at least temporarily, remedy boredom.

In this context, social engineering has the potential to also be understood as a practice of *detournement*—the subversive hijacking and flipping of conventional meaning best represented by "culture jammers and activists [who] diverted encoded scripts of obedience and consumption into invitations for innovation" (Ferrell, Hayward, & Young, 2008, p. 152). Social engineers take mundane business activities engaged in by corporate workers—sending emails about accounting, phone calls, walking into offices—and transform the meanings of these activities into illicit, and often illegal, undertakings that not only subvert, but also cut against the meaning of modern workplace life.

These perspectives highlight the relevance of focusing on the meaning and experience of emotion in attempting to understand phenomena such as social engineering. From the viewpoint of cultural criminology, felt experience may indicate acceptance of given cultural meanings, but it may also constitute a reaction to and rejection of established meaning. This work therefore emphasizes the significance that the structure of society and culture may have on the motivations inciting individuals to engage in social engineering, and the meanings and emotions expressed by an act of social engineering. By theoretically connecting culture to the emotions experienced in particular events, cultural criminology highlights the need to consider the ways in which the macro-level context may shape the experience of social engineering.

As social engineering is an interactional experience, using phenomenology, cultural criminology, and symbolic interactionism to approach this phenomenon will provide insight into the meanings and interpretations with which social engineers structure the experience. The affective dimensions of the experience may be shaped by and referential to broader understandings of social structure and culture, the social engineer's perceptions of self, and the social engineer's perception of the interaction and the others who are part of this interaction.

Maintaining Deceptions in Social Engineering

While the previous discussion focuses on the emotional experiences of social engineers as they engage in social engineering, the present section turns to an examination literature relevant to the second research question of the dissertation: the factors surrounding the maintenance of deceptions throughout social engineering attempts. In examining how social engineers maintain deceptions, the individual, organizational, and societal elements that are exploited may be revealed. Factors implicated in the literature on persuasion in social engineering are first reviewed Then, work on the role of communication mediums for deception and deception detection is reviewed. Lastly, a theoretical approach to analyzing the maintenance of social engineering deceptions is discussed.

Psychological perspectives on persuasion

Persuasive influences that occur in social engineering are a thread in the literature that provides insight into how social engineers are able to maintain deceptions without their targets being dissuaded as to the legitimacy of these deceptions. While this work on persuasion does not take a specifically interactional approach to social engineering deceptions, the findings can generally be applied to social engineering interactions. Much of the research and theoretical work on persuasion is influenced by social psychologist Robert Cialdini's (2008) framework of persuasion, which he first explicated in the 1980s based on his experience observing occupational positions involving marketing.

Robert Cialdini proposed six principles of persuasion, which are often used by social engineering studies to frame the abilities of social engineers to influence their targets (Applegate, 2009; Brody et al., 2012; Cialdini, 2008, Huang & Brockman, 2011; Workman, 2007; 2008). These principles, held by this perspective to be universal across cultures and interactions, are: reciprocity, authority, consistency, liking, consensus, and scarcity (Cialdini, 2008). The principle of reciprocity posits that people tend to feel an obligation to reciprocate gifts, favors, or positive social behaviors, such as invitations, that are given to them by others (Cialdini, 2008). It has been asserted that social engineers will use the persuasive influence involved in reciprocation to convince individuals to knowingly violate organizational policies in an effort to do a favor for the social engineer (Applegate, 2009; Brody et al., 2012; Workman, 2007). Reciprocation has also been linked to the concept of normative commitment, in which individuals feel obligated to adhere to the expectations produced by social norms regarding how to communicate and reciprocate to others (Workman, 2008). Normative commitment also plays a role in the persuasion principle of consensus, as individuals tend to engage in behaviors and have preferences of others similar to themselves (Workman, 2007).

Liking an individual is also theoretically associated with complying with the requests made by that individual (Cialdini, 2008). The likeability of a person is associated with similarity, as individuals like others similar to themselves, and so social engineers may intentionally draw comparisons between themselves and their targets in order to promote their influence over the target (Twitchell, 2009). In examinations of phishing emails, liking does not always appear as a common method of persuasion (Huang & Brockman, 2011). The persuasive principle capitalized on by a social engineer may be influenced by the type of fraud being attempted, however, as Whitty (2013) found that liking played a substantial role in persuading victims of online romance frauds to comply with the requests made by the social engineer.

Social engineers may also exploit the principle of consistency, also called commitment, which asserts that people prefer to act in ways consistent with their past behavior or claims. Bullée, Montoya, Pieters, Junger, and Hartel, (2018) suggest that social engineers may use this persuasion technique by repeatedly asking for increasing quantities of information from an individual who assented to revealing a minor amount of information until the social engineer gather enough information to compromise security. Scarcity is considered influential because the limited availability of a resource or opportunity may create a sense of urgency in individuals and increase their likelihood of pursuing scarce offers (Cialdini, 2008). This technique of influence in social engineering has been attributed to phishing emails, which may contain content that frames a situation as urgent and requiring immediate action on the part of the target (Huang & Brockman, 2011).

Authority is theorized as being persuasive, as individuals may be swayed by people who they perceive to be credible based on the institutional affiliations or social status of that individual (Cialdini, 2008). Huang and Brockman (2011) suggest that social engineers may claim false institutional affiliations in order to exploit this method of influence. For example, technical support telephone scams in which the social engineer attempts to gain access to the computer of a target by suggesting that the computer has a virus may intentionally invoke the company name Microsoft in an effort to appear as knowledgeable experts with a credible institutional affiliation. Empirical examinations of the role of authority in social engineering have derived mixed conclusions about the applicability of this form of persuasion. On one hand, authority is a persuasive technique that is frequently attempted in social engineering. Emails endeavoring to defraud victims have been found to commonly employ authority as a persuasive method (Huang & Brockman, 2011). The use of authority is also apparent in the analysis by Bullée et al. (2018) of 74 social engineering engagement narratives from 4 published books on social engineering. Out of the 6 principles of persuasion, authority made up 63.3 percent of the occurrences of persuasion that occurred during the social engineering descriptions (Bullée et al., 2018).

Although authority may be found to commonly transpire in social engineering, the frequency of occurrence is not necessarily associated with the efficacy of this techniques. In fact, a study of the effect of authority in face-to-face social engineering found that individuals exposed to the authority persuasion condition were not significantly more susceptible to social engineering than those in the control group (Bullée, Montoya, Pieters, Junger, & Hartel, 2015). It should be noted, however, that the use of authority in this study was operationalized through the social engineer wearing business clothing versus casual clothing, which may not convey authority sufficiently enough to be persuasive. In contrast, Whitty (2013) provides some indication that authority may play a role in social engineering success. This study interviewed victims of online romance scams and found that the social status and institutional affiliations feigned by the social engineer were qualities that led the victim to feel that the scammer was trustworthy (Whitty, 2013). It may also be that the authority of the target of social engineering, in addition to the authority of the social engineer, may impact social engineering susceptibility. This finding is suggested by Aurigemma and Mattson (2017) who discovered that high organizational status and perceived ability to control coworker behavior was associated with employee willingness to prevent tailgating from occurring.

As evinced here, scholars contend that social engineers may draw on a range of these persuasive principles in an effort to maintain a deception. Which persuasive principles are employed by the social engineer is likely to be contingent on the individual preferences of the social engineer, as well as the situational context in which the attempt is occurring. One factor of the situational context which may be consequential for the way in which social engineers attempt to maintain deceptions is the communication medium in which the deception is being conveyed.

Communication Medium and Deception

In both theoretical and experimental literature, communication medium is implicated in both the structure of interactions, as well as the way in which deception occurs. While social theorists, such as Goffman (1956) and Giddens (1990), have tended to specify the face-to-face dimension of social interaction as their central focus, other works examine the differences in experiences of social interaction across different mediums of communication. The role of interaction across technological communication mediums has been considered across various contexts of e-commerce, from eBay transactions (Resnick & Zeckhauser, 2002), to mechanisms that reduce the possibility of deception on platforms that facilitate the sharing economy (Etzioni, 2019), to consumer trust in buying illegal goods and services from darkmarket forums (e.g. Dupont, Côté, Savine, & Décary-Hétu, 2016; Holt & Lampke, 2010; Leukfeldt, Kleemans, & Stol, 2017; Lusthaus, 2012; Yip, Webber & Shadbolt, 2013) to deception of online customers (Grazioli & Jarvenpaa, 2000). Interactions across mediated communication in the context of commerce differs in important ways from social engineering deceptions across mediated communication. Specifically, the consumer in these contexts knows that they are entering into a transactional interaction, and these interactions are therefore relegated to issues such as payment, product acquisition, and product quality. In contrast, the social engineer may attempt to maintain a deception during a social engineering engagement regarding the fundamental purpose of the interaction itself. In addition, circumstances in which social engineering deceptions take place widely vary. For this reason, this review will focus on the impact of communication mediums on trusting information presented as true, and the success and failure of the maintenance of deceptions broadly, rather than provide an in-depth examination of interactions across commerce interactions.

These differences are particularly relevant to experiences of social engineering, as social engineering may occur across many forms of communication. The extent to which the communication is documented, the synchronicity of the communication, and the separation in space between interacting individuals are all qualities of communication that may transform the experience of interacting with another individual (Hancock, 2012). For example, interactions that occur asynchronously between distant individuals may allow individuals who would be unable to engage in expressive control during face-to-face interactions to instead maintain a coherent presentation of who they present themselves to be (Goffman, 1956).

Computer mediated communication (CMC), or technology mediated communication, such as through email, online message forums, or other forms of messaging, has been found to have both interactional differences and similarities with face-to-face communication. Aspects of both the content of communication and acceptable interactional behavior may differ from face-to-face communication in CMC. Tong and Walther (2015) argue that because CMC has fewer channels through which individuals can convey information through interaction, each participant has greater control over presentation of self, and a greater ability to communication without sending conflicting signals. Similarly, the amount of time a person may take to craft a written message across CMC, as well as the ability to edit text prior to communication, is suggested to promote the extent to which impression management and self-presentation can be controlled across CMC (Walther, 2007). Even when individuals could see each other through video feeds, individuals using CMC who were meeting for the first time would ask more questions and engage in more intimate disclose than individuals meeting face-to-face (Antheunis, Schouten, Valkenburg, & Peter, 2012). Remaining silent and not acknowledging asynchronous messages, such as email, may also be considered a valid option, as opposed to the norms of in-person social interaction (Tong & Walther, 2010).

There are other similarities across dimensions of communication. In both face-to-face communication and through CMC, disclosure of personal information to individuals was found to promote liking from those individuals (Kashian, Jang, Shin, Dai, & Walther, 2017). Individuals also took social norms into account when rejecting romantic interest from those who they had previously met and thought they might interact with in the future (Tong & Walther, 2010).

A factor that differentiates the maintaining deceptions during social engineering attacks across CMC is the increased potential of employing automated detection methods to evaluate these communications. Machine learning models have been used to evaluate deceptive identities of accounts on Twitter (van der Walt, Eloff, & Grobler, 2018). The linguistic characteristics of deceptive emails between business partners have been analyzed for the purpose of evaluating the usefulness of automated text analysis in email (Ludwig, Van Laer, Ruyter, Friedman, 2016).

The nature of deceptive interactions also appears to differ across forms of communication. Van Swol, Braun, and Kolb (2015) conducted a study of deception in a game they designed for participants. They found that types of deception differed between these two forms of communication. Specifically, the authors discovered that more overt lies were employed as a deceptive strategy in CMC communications, while face-to-face deceptions occurred more through the omission of information. Rates of deception were not found to vary significantly, however, between communication conditions, nor did truth bias differ between these conditions (Van Swol, Braun, & Kolb, 2015).

Whether or not the ability to maintain deceptions is impacted by communication medium is uncertain, as studies reach ambiguous and contrasting conclusions. Research has found that accurate detection of deception, and therefore the failure to maintain the deception, was significantly higher for participants using CMC than face-to-face communication (Van Swol, Braun, & Kolb, 2015). On the other hand, Hancock, Woodworth, and Goorha (2010) found no main effect between communication medium and deception detection, although motivated deceivers using CMC were found to have significantly higher rates of successful deceptions.

Differing strategies to counter the maintenance of deceptions across varying mediums of communication is attributed to the differences in the types of information that can be used to evaluate the legitimacy of information conveyed across these mediums. It has been noted that the nonverbal aspect of communication is both influential in how people evaluate deceptions, and that this dimension of communication is absent in most forms of CMC (Hancock, Woodworth, & Goorah, 2009; Pak & Zhou, 2014; Van Swol, Braun, & Kolb, 2015). Bond and Depaulo (2006) conducted a meta-analysis and discovered that the ability to accurately discriminate between truth and lies was lower for participants who viewed video footage alone, and had to make decisions based purely off of nonverbal communication, but that the difference in accurate determination between truth and lies did not differ for participants who made decisions based on audiovisual information, audio alone, or written transcripts alone. The results of this area of research indicate that social engineers may attempt to utilize mediated forms of communications to counter conveying information that could lead to the failure to maintain a deception.

Maintenance of Deceptions in Social Engineering: Theoretical Approach

This section builds on the findings of the academic literature to describe the theoretical approach that will be used to examine the ways in which social engineers maintain deceptions. The research question used in the analysis is: *How do social engineers attempt to maintain deceptions while engaging in social engineering?* This research question is contextualized within a theoretical approach focused on interactional context, social structures, and mediated communication on the ability of social engineers to maintain deceptions while engaging in social engineering.

Insights can be gleaned by approaching deceptions in social engineering attempts from an interactionist standpoint that extend beyond the extant findings of research on persuasions in social engineering. Goffman (1956), demonstrates the reciprocal exchange that occurs over the course of an interaction, as individuals work to convey information about an individualized and subjective perception of reality to one another. Social engineers must maintain deceptions across this dynamic series of exchanges, which will be examined in the analysis of this research question.

Exploring the interactionist dimensions of maintaining deceptions in social engineering may also be revelatory of the ways in which social engineers exploit social systems and institutions Giddens (1990) draws on Goffman (1967) and connects the micro-level analysis of interaction back to a macro-level analysis of society in modernity by discussing facework commitments and faceless commitments. These two commitments both rely on trust in a narrative that is being presented as true. In facework commitments, the trust is that an individual is communicating truthfully, which is maintained by social rituals in interaction. Faceless commitments, in contrast, are characterized by a reliance on abstract systems to determine reality.

The sociological theory of modernity developed by Giddens (1990) explicates the form that trust takes in the modern context and its role in the formation and maintenance of present day social institutions. Within this perspective, one of the fundamental characteristics of modernity is that social relations become disembedded from local contexts—that interactions are no longer bounded within particular places and timeframes (Giddens, 1990, p. 21). The role of the disembedding mechanism of expert systems is especially relevant the maintenance of deceptions in social engineering, which requires reliance on expertise of others often without having personal knowledge of either the other upon whom one relies or knowledge of the area of expertise. Expert systems encapsulate "systems of technical accomplishment or professional expertise that organize large areas of the material and social environments in which we live today" (Giddens, 1990, p. 27). A feature of this disembedded character of modernity is therefore that individuals are continuously reliant on expert systems, often divorced from any knowledge of the competence of the particular individuals involved within the system. For example, people regularly venture onto airplanes without questioning the competence of the pilot or the abilities of the aircraft mechanics, instead trusting that policies and regulatory organizations have vetted the individuals upon whom the fliers rely.

A crucial component of abstract systems is that they imply a default assumption of legitimacy from the individuals who interact with them (Giddens, 1990, p. 27). A gap exists between the knowledge possessed by the individual, and the expertise provided by the expert system of which the individual is often ignorant. This gap in knowledge, which necessitates trust, may be exploited by social engineers who maintain deceptions in which they fraudulently represent themselves as being part of these expert systems.

The role of different mediums of communication in shaping how are maintained also has theoretical implications for social engineering. As varying forms of communication can be used to examine different aspects of the communication for signs of veracity, so to can these communications be used to disguise varying aspects of the deception that is being perpetrated (Walther, 2007). Social engineering involves deceptions that cut across communication mediums—occurring in email, over the phone, through text, and in-person, among other potential communication methods.

Deception Detection in Social Engineering and Security Awareness

Social engineers are not always successful in their attempts to maintain deceptions in social engineering attempts, but may instead be detected by the targets they sought to deceive. This potential for deception detection to occur within a social engineering occurrence will be the third research question to be explored by this dissertation, and therefore relevant literature on this topic will be examined in this section. The field of deception detection has extensively studied a wide range of situations in which deceptions may be detected, and serves to contextualize how deception detection takes place within social engineering. This review begins by examining the phenomenon of deception and contextualizing the occurrence of social engineering as part of deceptive practices that have occurred throughout history. Turning to the field of deception detection, literature which explores how potential deception, and the detection of such deception, occurs as an interaction between two or more people who are in interaction with one another. The review then outlines perspectives from the literature on the potential role of psychology and cognition in impacting the detection abilities of individuals. Lastly, the theoretical considerations of deception detection are considered in this section.

Establishing the Phenomenon

In 1837, having witnessed the societal upheaval caused by the technological transformation of the Industrial Revolution, Englishman Richard Alfred Davenport opened his book *Sketches of Imposture, Deception, and Credulity* with these words:

> Incredulity has been said, by Aristotle, to be the foundation of all wisdom. The truth of this assertion might safely be disputed; but, on the other hand, to say that credulity is the foundation of all folly, is an assertion more consonant to experience and may be readily more admitted: and the contemplation of this subject forms a curious chapter in the history of the human mind (p. 1).

Davenport (1837) then embarks on writing a chronicle of the vast array of deceiving situations and impostures that have hoodwinked people throughout history. While Davenport is no doubt in large part writing for the entertainment of his audience, the self-proclaimed purpose of the work is to "show that the credulity of the many—in some cases synonymous with the foolish—has been, from the beginning, most readily imposed upon by the clever and designing few" (p. 2). Staunchly an Enlightenment man, Davenport reflects back on the past and sees the ease with which people trusted and were duped as a consequence of a lack of knowledge and an absence of rational thought. Looking forward from his situated stance in 1837, he envisioned a new era of scientific knowledge in which people would be more firmly grounded in a foundation of rational knowledge and better able to be incredulous of disingenuous representations made by others.

Putting aside Davenport's quixotic optimism, a similar emphasis on considerations of how people assess the trustworthiness of other individuals and social institutions came to prominence in the works of sociologists and other theorists considering the structure of modernity at the end of the 20th century. While these theorists elucidate different dimensions of society in their development of these concepts, they can be understood as similarly grappling with the restructuring of society in the Digital Revolution. Giddens (1990), a prominent scholar in this area, explicitly conceptualizes trust and knowledge as distinctively intertwined within the conditions of modernity (pp. 34-35).

This awareness and focus on social engineering in the context of information security is fundamentally a concern with how human credulity and trust are susceptible to deception and the ensuing consequences of interacting with others from a trusting stance when the valid response should have been skepticism. Considerations of trust are additionally complicated in this context, as targets of social engineering are often individuals who are interacting with or working within informated organizations. These targets therefore exist in a context in which the evaluation of potential deceptions often relies on knowledge of how to appropriately use and interact with technologies and data.

The present literature which concerned with the susceptibility of individuals to deceptions, as well as their ability to detect deceptions, is examined by research on deception and social engineering. Much of this literature examines social engineering victims from a deficits-based perspective; attempting to discern factors that make individuals susceptible to persuasion by social engineers. The following section will present the literature on susceptibility to persuasion, due to its significance in this academic area, before turning to the work from the field of deception detection. Then, a theoretical examination of deception detection in social engineering will be discussed.

Susceptibility to Persuasion & Deception

Much of the extant research considering individual susceptibility to persuasion from social engineers relies on the wholesale transfer of perspectives from social psychology onto the phenomenon of social engineering. The empirical evaluations of these psychological concepts often come to inconclusive or inconsistent conclusions about the impact that they have regarding social engineering. This point is noted by Norris, Brookes, and Dowell (2019) in a review of the literature on the psychology of victimization from internet fraud, as they assert that the current research on the matter stands “still some way from achieving a robust and testable model on online fraud susceptibility” (p. 232). Furthermore, couching social engineering susceptibility in psychological terms overlooks the interactional process and experience of social engineers to effectively implement persuasive situations as well as skirts over the security awareness strategies engaged in by potential victims to evaluate and evade situations in which they could be deceived and exploited.

Psychological attributes of victims. In addition to examining the ways in which persuasion occurs in the context of social engineering, research has also explored various psychological traits of victims said to be exploited by social engineers. These traits include personality traits possessed by the victims, victim emotions, and dispositional characteristics. In particular, victim disposition to trust and victim disposition to risk have been considered with regards to social engineering.

A psychological factor that has been examined in this literature are how personality traits are influential in relation to social engineering. Curtis, Rajivan, Jones, and Gonzalez (2018) examined the association between personality traits and the ability to correctly identify phishing and non-phishing emails and found that participants with higher levels of narcissism were significantly more vulnerable to phishing emails. The authors suggest that this finding may be attributable to an association between narcissism and overconfidence in ability, as well as impulsivity. Both agreeableness and extraversion were found to be associated with social engineering susceptibility out of the Big Five personality traits by Cusack and Adedokun (2018), while Lawson, Zielinska, Pearson, and Mayhorn (2017) found only extraversion to be associated with susceptibility to phishing emails.

Psychological characteristics of victims that have been implicated in social engineering include the disposition to trust, which refers to the tendency of an individual to believe others across interactional situations, has been suggested to promote susceptibility to social engineering victimization (Luo, Brody, Seazzu, & Burd, 2011; Williams, Beardmore, & Joinson, 2017; Wright & Marett, 2010). Individuals who are more inclined to trust other people with whom they interact may also be more susceptible to truth bias, which refers to the propensity of people to assume that others, especially trusted others, are telling them the truth (Twitchell, 2009). Dispositional responses to perceived risk are also suggested to be related to social engineering victimization susceptibility, as individuals who discount the extent and impact of information security threats may be more likely to become victims of social engineering (Aleroud & Zhou, 2017; Wright & Marett, 2010).

The research that has examined these dispositional attributes has arrived at contrasting results. Disposition toward trust and risk were both found to be significantly associated with phishing email susceptibility by Workman (2007). More trusting individuals were found to be more likely to respond to phishing emails than less trusting individuals, while individuals who perceived phishing emails as risky were less likely to fall victim to these emails than those who perceived the phishing emails as posing a severe risk (Workman, 2007). Perceived risk has also been found to be associated with precautionary behaviors on social media websites, such as having higher privacy and security settings (van Schaik, Jansen, Onibokun, Camp, & Kusev, 2018). In contrast, another study of phishing emails by Wright and Marett (2010) found that perception of risk and disposition to trust were not associated with susceptibility to being deceived by a phishing email. This study did find that suspicion of humanity, which was conceptualized as a distinct construct from disposition to trust, was associated with resistance to phishing deceptions.

Strong emotions, such as fear and anger, may also be used by social engineers to overload targets and reduce the targets' ability to evaluate the legitimacy of the social engineer and the requests made by the social engineer (Indrajit, 2017; Twitchell, 2009; Workman, 2008). Impulses with strong affective aspects, such as curiosity and greed, are also characterized as conduits that social engineers can use to exploit their victims (Abraham & Chengalur-Smith, 2010). Despite these postulations, it has been observed by Williams, Beardmore, and Joinson (2017) that "the impact of emotions on responding to online scams has been largely neglected" (p. 416). This observation could be extended beyond the specificity of online scams to include other forms of social engineering, as the impact of emotions in social engineering attempts across any means of communication has been mostly lacking.

Extending beyond purely psychological perspectives of social engineering victimization, there is a small, but growing, body of research on experiences and perceptions of online fraud victimization within criminology (e.g. Cross, 2015; 2016; Whitty, 2013; Whitty & Buchanan, 2016). Research on internet romance frauds, in particular, has examined elements of the emotional experience of the victims of such frauds (Gillespie, 2017). The emotional dimensions of this type of fraud are especially prominent, as the scam entails that the social engineer communicates with a victim, often for extended periods of time, to establish a false romantic relationship with the victim and use the ensuing emotional connection to request money under false pretenses (Kopp, Layton, Sillitoe, & Gondal, 2015). Whitty and Buchanan (2016) note that when the victims of the fraud become aware that they have been scammed, they experience intense negative emotions such as fear and anger over their financial loss, but often more importantly, over the loss of a previously valued relationship. Whitty (2013) also notes that romance scams often have an initial euphoric stage as the scammer initiates a romantic relationship with the victim, which then turns to a victim experience of anxiety and stress as the scammer concocts a tale of financial need to extract money from the victim.

Research on Deception Detection

In contrast to examining factors that may produce susceptibility to social engineering deceptions, deception detection research focuses on factors related to the ability to discern when such deceptions are taking place. Deception detection is an interdisciplinary field of study, centered in communications studies, and, adjacently, psychology, that examines how deceptions are created, conveyed, and evaluated by taking into account the communicator of the deception, the receiver of the deceptive communication, and the content and context of the interactional situation (Depaulo, Ansfield, & Bell, 1996). Various scholars within communication studies have attempted to conceptualize, theorize, and synthesize the components of the processes of interpersonal deception (e.g. Buller & Burgoon, 1996; Depaulo, Ansfield, & Bell, 1996; Levine, 2014; Levine & McCornack, 1991; 2014; Park, Levine, McCornack, Morrison & Ferrara, 2002). Most research that empirically examines deception detection does so in experimental settings or in situations related to law enforcement, therefore examining social engineering in the context of deception detection stands as a unique contribution to this area of research. Furthermore, little literature that focuses on deception detection examines perceptions of the interactional process of navigating deceptive interactions across varying forms of communication.

One of the most persistent findings established by the deception detection literature is that, for the most part, humans are unable to successfully detect deceptions at a rate higher than could be attributed to chance, across a variety of conditions (Bond & DePaulo, 2006; Burgoon, Buller, Ebes & Rockwell, 1994; Levine & McCornack, 2014; Wright, Berry & Bird, 2012). This finding is partially accounted for by another consistent finding: the existence of truth bias in deception determinations (Buller & Burgoon, 1996; Burgoon, Buller, Ebesc & Rockwell, 1994; Levine & McCornack, 1992; Stewart, Wright & Atherton, 2019; Van Swol, Braun, & Kolb, 2015). Truth bias refers to the inclination of people to generally be trustful that the information communicated to them by another individual is truthful, even when they have been alerted to the potential for deception to occur (ibid).

A contrasting finding to the occurrence of truth bias is what Meissner and Kassin (2002) term *investigator bias* in a study which found that video interviews of suspects were determined to contain deceit at higher rates according to police investigators than according to college students who viewed the tapes. Additionally, police investigators who had received professional training on interrogations and deception detection were evaluated these interviews as deceitful significantly more than did police investigators who had not received such training. Notably, those who impugned the veracity of the interviews at higher rates were *not* substantially more accurate in their ability to correctly classify interviews as either deceitful or truthful (Meissner & Kassin, 2002). These findings regarding both truth bias and investigator bias suggest that, regardless of the inclination to find communications truthful or deceitful, human ability to discern deceitfulness is lacking.

One finding that might inform understandings of the difficulty that people have in accurately detecting deception emerges from research regarding the unreliability of deception cues that are used to evaluate whether or not information is deceptive (Levine, 2014; Qin & Burgoon, 2007). Levine and McCornack (2014) assert strongly that deception detection has consistently “failed to identify reliable behavioral cues that differentiate between honest and deceptive communication” (p. 432). A variety of cues have been theorized to be associated with deceptive communications; often broadly categorized as verbal deception cues and nonverbal deception cues (Buller & Burgoon, 1996; Frank, Menasco & O'Sullivan, 2008; Hamlin, Wright, Van der Zee, & Wilson, 2018). Many different verbal deception cues have been examined, a few of which include the use of filler words (i.e. ‘um’, ‘like’, ‘hm’) (Arciuli, Mallard, & Villar, 2010), variation in the use of personal pronouns or active verbs (sometimes called ‘non-immediacy’) (Burgoon, Buller, White, Afifi & Buslig, 1999; Zhou & Zhang, 2008), and rate of speech (Evans, Michael, Meissner & Brandon, 2013). Non-verbal cues in the research that have been examined include the extent to which the potential deceiver makes eye contact (Qin & Burgoon, 2007), facial ‘micro-expressions,’ gestures, and bodily posture (Bond & Depaulo, 2006; Ekman & Friesen, 1969; Hamlin, Wright, Van der Zee, & Wilson, 2018), as well as the extent to which the communicator is perceived as having an ‘honest demeanor’ (Levine, et al., 2011).

The inability to reliably use verbal and non-verbal cues to detect deceptive communication has been imputed to features of both the senders of the deceptive communications as well as to the receivers of the messages who are attempting to determine veracity. Regarding the senders, Levine (2010) argues that while most deceivers provide scant clues to divulge their deception, it is possible that a small fraction of these individuals may emit deception cues that are readily interpreted as signs of duplicity. Some researchers argue that the motivations behind the deceptions, the deceiver’s perception that deception involves high stakes, or the deceivers' social skills, impacts their emotional arousal and heightens the expression of deception cues (Bond & DePaulo, 2006; Buller & Burgoon, 1996; Hancock, Woodworth & Goorah, 2010; Porter, McCabe, Woodworth, Peace, 2007), while others dispute this supposition (Levine & McCornack, 2014).

Putting aside the potential variations in the deceptive efficacy of deceivers, research further reveals the interpretation of cues as indicative of potential deceptions are often unrelated to the actual occurrence of a deception. For example, Bond et al. (1992) created video footage of people sitting and telling the truth about their feelings and footage of them lying about their feelings, then also created videos the same footage, except the people engaged in a nonverbal behavior that violated social expectations (e.g., keeping eyes closed, raising one hand above their heads) while they gave their true or false descriptions. Participants who viewed this footage without sound, tended to infer deception from the footage of the subjects engaging in norm-violating behavior.

These findings also occur when participants do not have to rely entirely on nonverbal cues. Levine, et al. (2011) found that demeanor, defined as "the believability of the message sender independent of actual honesty" (p. 379), explained a large portion of whether participants decided a message was deceptive or not, independent of message veracity. The interpretation of the same cues may also differ, as found by Granhag and Strömwall (2000), who conducted an experiment in which participants evaluated the truthfulness of the same video footage of testimony given by a witness. They found that participants both had divergent perceptions of whether or not the witness offered consistent statements across the testimony, and differed in their interpretations as to whether or not consistency, or lack thereof, was demonstrative of deception (Granhag & Strömwall, 2000).

Various dimensions of knowledge have also been examined with regards to their potential influence on the outcomes of attempted deception detection. In this context, the knowledge being examined tends to be that of the person making the decision about the veracity of a communication, rather than that of the deceiver. Specifically, the knowledge that comes from expertise and training of deception detection techniques has been examined. Training people to evaluate nonverbal information for signs of deception is suggested to be ineffective (Hauch, Sporer, Michael, & Meissner, 2014), though some studies suggest that training in asking strategic questions may increase deception detection (Levine, 2014; Vrij, Granhag, Mann, & Leal, 2011), though the effect of these trainings may be the result of evaluating information more critically, rather than due to any useful knowledge provided by the training (Levine, Feeley, McCornack, Hughes & Harms, 2005). Blair, Levine, and Shaw (2010) evaluated the ways in which knowledge of context increased deception detection accuracy, and argue that knowledge of situational context is more representative of how people make real-world decisions about deception. This argument is bolstered by the findings of Park, Levine, McCornack, Morrison, and Ferrara (2002) who studied how people discovered deceptions in their daily lives and found that most deceptions were revealed through third-party information or physical evidence. Domain knowledge of social engineering and cyber-security has also been specifically implicated in the ability to detect and contend against these deceptions (Ben-Asher & Gonzalez, 2015; Campbell, 2018).

Trust and suspicion have also been taken up by deception detection research. It has been posited truth bias can be attributed to a default trusting orientation that undergirds societal cohesion (Buller & Burgoon, 1996; Kim & Levine, 2011; Levine et al., 2011). This conceptualization of trust is bolstered by findings that individuals judge people with whom they had a prior relationship more truthful than strangers (Buller, Burgoon, Buslig, & Roiger, 1996), and that people are better at detecting deceptions by observing conversations than by participating in those conversations (Buller, Strzyzewski, & Hunsaker, 1991).

Empirical research has examined how people evaluate deceptions under different suspicion conditions. Levine and McCornack (1991) found that people with a higher "predisposition toward believing that the messages produced by others are deceptive" (p. 328) were more likely to evaluate the communications in their study as deceptive, but also that people with low levels of this predisposition who had been put into a state of suspicion by being warned of the potential for deception were also more likely to evaluate communications as deceptive. Research on the demeanor of potential deceivers is evaluated as a deception cue connects interpretations of demeanor to evaluations as to whether the communicator is trustworthy or suspicious (Levine et al., 2011). Examinations of the moods of people making deception detection decisions finds that people in negative moods are more likely to evaluate communications as deceptive (Forgas & East, 2008). Although suspicion is associated with higher rates of evaluating communication as deceptive, it is not associated with increased accuracy in being able to discern which communications are truthful and which are deceptive (Kim & Levine, 2011).

The deception detection findings on trust and suspicion also have specific implications for social engineering deceptions, both in-person and over various forms of mediated communication. Social media platforms have been theorized to produce trust and relational ties between strangers who would be otherwise unconnected, promoting the possible situations in which social engineering could occur or information could be exploited for social engineering purposes (van der Walt, Eloff, & Grobler, 2018). Campbell (2018) asserts that people and businesses may be susceptible to social engineering because individuals in organizations by default trust automated information and digital communications. Lastly, social engineering may exploit how people evaluate the credibility of websites, phone applications, and the communications that occur on these platforms (George, Giordano, & Tilley, 2016; Grazioli, & Jarvenpaa, 2000).

Deception Detection in Social Engineering: Theoretical Approach

The theoretical insights derived from the deception detection literature may provide insight into the third analysis within this dissertation: *How does deception detection occur in social engineering interactions?* An examination of social engineering in the context of deception detection research may be revelatory of both the ways in which both social engineers and the targets of social engineering perceive the relevant factors related to detecting social engineering deceptions. Although not all deceivers are social engineers, all social engineers are deceivers. The deceptions practiced by social engineers have characteristic features that may separate social engineering as a subset of deception as a whole. First, social engineers are attempting to deceive individuals with whom they do not possess a prior acquaintance. Second, the deceptions made by social engineers are more substantial than the everyday social deceptions people engage in, such as lies told about feelings about a situation (DePaulo, Kirkendol, Kashy, Wyer, & Epstein, 1996). Third, social engineers enter into situations with the foreknowledge that these situations will involve deception, in contrast to deceivers who find themselves unwilling to disclose information in the midst of a conversation and therefore insert deception without prior intention (McCornack, Morrison, Paik, Wisner, & Zhu, 2014).

Several findings from the deception detection literature may be of relevant here, including truth bias (Stewart, Wright & Atherton, 2019; Van Swol, Braun, & Kolb, 2015), leakage of verbal and nonverbal cues (Bond & DePaulo, 2006; Buller & Burgoon, 1996), and contextual information (Park, Levine, McCornack, Morrison, and Ferrara, 2002).

The deception detection literature also highlights the potential roles of knowledge, trust, and suspicion in the detection of deceptions (Buller & Burgoon, 1996; Campbell, 2018; Levine et al., 2011). The importance of trust in this work can be theoretically bolstered by the incorporation of sociological conceptualizations of trust that may play a role in the success of social engineering deceptions.

Trust has been attributed to being the basis of social order, necessary for the functioning of organizations, and fundamental to interpersonal interactions. Both the affective aspects of trust as well as the cognitive dimensions have been emphasized and examined (Jones, 1996; Lewis & Weigert, 1985). An assumed prerequisite for trust is the initiation of an interaction in which at least one actor must rely on, and place trust in, the other in the interaction (Gillespie, 2007).

Conclusion

The use of social engineering frauds to deceive individuals and organizations has remained a persistent threat throughout social and technological changes over recent decades. As a result, scholarly focus on this phenomenon has increased in recent years (Yasin, Fatima, Liu, Yasin, & Wang, 2019). The research produced in this area primarily focuses on issues such as, the techniques used in social engineering attacks, psychological factors exploited by the social engineer, and persuasion principles used in social engineering (Yasin, et al., 2019). Notably, little research exists on the social engineers themselves—from their demographic characteristics, to what motivates them, how they are situated in economic and cultural structures, how they perceive and experience their engagement in social engineering deceptions, and how they understand their targets. Older work that examines fraudsters and their experiences indicates that examining the aforementioned factors is revelatory of the motivations and circumstances that promote the perpetration of these frauds (e.g. Doocy, Shichor, Sechrest, & Geis, 2008; Jackson, 1994; Shover, Coffey & Hobbs, 2003; Sutherland, 1937/1989). Thus, this dissertation seeks to contribute to an understanding of the perpetrators of social engineering deceptions by examining the question: *What are the experiential dimensions of engaging in social engineering?*

Although social engineering is often noted to exploit human beings to compromise security (e.g. Archchilage & Love, 2014; Brody, Brizzee, & Cano, 2012; Cox, 2012; Hu, Diev, Hart & Cooke, 2012; Luo, Brody, Seazzu, & Burd, 2011; Tsohou, Karyda, & Kokolakis, 2015; van Schaik, et al., 2017), the work in this area tends to overlook the dynamic interactional deception process that occurs in social engineering attacks. Deception detection theorists and researchers have situated deception within interactions in which deceivers "control the information in their messages to depart from the truth as they know it" (Buller & Burgoon, 1996, p. 205), while the receivers of such messages evaluate these communications and derive conclusions regarding the veracity of the content of the message, and the interaction as a whole (Buller & Burgoon, 1996). This interactional approach to deception provides a unique lens for understanding the ways in which social engineering deception can be detected and evaded by potential victims. This dissertation will, therefore, examine the question: *How does deception detection occur across social engineering interactions?*

Lastly, the ways in which social engineers maintain deceptions in the course of social engineering provides insight into the scaffolding that undergirds the entirety of the social engineering attempt. While theorists, such as Cialdini (2008), have provided indications of the methods and strategies used to persuade targets to accept fabrications as valid, the interactional process that a social engineer enters into has yet to be explored. Therefore, this dissertation analyzes the question *How do social engineers attempt to maintain deceptions while engaging in social engineering?*

Chapter 3 - Methods

This dissertation examined the previously discussed research questions through qualitative interviews with social engineers, security auditors, and IT professionals. As these research questions seek to investigate issues related to people's perceptions, beliefs, experiences, and constructs of phenomenon, a qualitative methodology is an appropriate approach for this research (Berg, 2004). Specifically, for the research question "*What are the experiential dimensions of engaging in social engineering?"* a qualitative approach is beneficial (Corbin & Strauss, 2015) because this question is focused on the subjective, inner experiences of social engineers. Examining the narratives of social engineers in this context provides insight into their experiences and the meanings by which they approach these encounters. The research question "*How does deception detection occur across social engineering interactions?"* is likewise best analyzed from a qualitive stance to capture the dynamic negotiation of meanings that characterize the process of human communicative interactions (Lindlof & Taylor, 2019). Lastly, the research question *"How do social engineers attempt to maintain deceptions while engaging in social engineering?"* explores the experiences and beliefs of social engineers as they seek to accomplish the goals of their social engineering endeavors. As qualitative research methods provide a means of analyzing the dimensions of abstract constructs, this will be the methodology used to examine this last research question (Berg, 2004).

Sample

The data for the dissertation consisted of interviews with 54 participants who were recruited and as part of a National Science Foundation-funded research project [grant number SES-1616804] that interviewed social engineers, security auditors, and information technology professionals who work to secure organizations from social engineering threats.

Participant recruitment involved a mix of purposive and snowball sampling strategies. Purposive sampling is used to recruit members from specialized populations who have relevant knowledge or expertise on a topic that is relevant to the research questions of a study (Berg & Lune, 2012, Lindlof & Taylor, 2019). Esterberg (2002) recommends this purposive sampling strategies for qualitative research as choosing participants for the specific knowledge and perspectives they provide "can give you the greatest possible insight into your topic" (p. 93). This form of sampling strategy, while limiting generalizability, allows qualitative research to reach an in-depth understanding of a phenomenon situated in a particular context (Esterberg, 2002; Lindlof & Taylor, 2019). As knowledge and experiences of social engineering and security awareness is specialized to particular groups, such as IT professionals and social engineers, this sampling strategy is appropriate for the current research topics.

Snowball sampling is a strategy that relies on referrals to the researcher (Esterberg, 2002; Lindlof & Taylor, 2019). This form of sampling may occur when one participant in a study refers the researcher to another participant who possesses attributes relevant to the research topic (Lindlof & Taylor, 2019). Snowball sampling can also occur if a request for interviews is circulated through a group of potential participants, such as through emails being forwarded to an email list (Esterberg, 2002). This process is called snowball sampling, as "The chain of referral creates an expanding pool of respondents—a "snowball" growing larger over time" (Lindlof & Taylor, 2019, p.148). This form of sampling is frequently used for hard-to-access populations, such as individuals in criminal subcultures, as well as in other situations where gaining access poses a research challenge (Esterberg, 2002). As social engineers may be engaged in illegal or socially deviant activities, this population is best accessed through a snowball sampling strategy. IT professionals may likewise difficult to access due to organizational restrictions on speaking about security policies and sensitivity surrounding discussions of security breaches.

Purposive sampling strategies were used to recruit IT professionals, security auditors, and social engineers. Both social engineers and security auditors were recruited from professional conferences. The researchers also cold-called information security contractors claiming to offer social engineering penetration testing services identified through internet search engines. Finally, participants were also recruited through snowball sampling by participants providing references to others possible interview participants.

Generalizability

The use of non-random sampling in qualitative research raises the question of generalizability—to what extent do the experiences and knowledge conveyed by the 54 participants in this dissertation represent social engineers and IT professionals as a population? Prior to delving into the specific sample used in this dissertation, the question will first be framed in the context of generalizability within qualitative research as a methodology. Limitations of the sample and directions for future research will also be discussed in-depth in the Conclusion section of the dissertation.

In examining generalizability, it important to distinguish both the methods and results of qualitative research from that of quantitative research. Concerns with sampling selection in quantitative research is due to the importance of sampling distributions in conducting inferential statistical analysis that allows a researcher to generalize from a sample to the population (Babbie, 2013, p. 198). In contrast, the results of qualitative research elucidate subjective meaning structures, which can allow the researcher to conceptualize aspects of social life and social structures[3], as well as engage in theory-building (Katz, 2001; Weiss, 1995). Thus, in qualitative research, generalizability is achieved by analyzing data with sufficient variation and range to capture the breadth of the phenomenon that is under examination (Katz, 2001a; Stinchcombe, 2005; Weiss, 1995). As Weiss, (1995, p. 24) states, "One argument for generalizing to a larger population from a sample chosen to maximize range depends on being able to claim that the sample included the full variety of instances that would be encountered anywhere." Only in interrogating the data across a wide variation of cases or events, can a generalizable description be arrived at of the framework that structures social life.

Returning to the specific sample of 54 participant interviews in this dissertation, it is undoubtedly the case that areas of the data exist which are missing the full range of human experience that constitutes that phenomenon under investigation. For example, all the participants in the study were based in English-speaking countries, primarily the United States, which means the results of the qualitative analysis will be structured within a cultural and historical context that may fail to be generalizable to other countries and cultures. Additionally, certain subsets of social engineers, such as professional criminals involved in organized crime, are absent from the sample. The results of this dissertation, therefore, is likely to fail to be representative of the experiences of social engineers who engage in social engineering in a context that substantially differs from that of the participants interviewed for this research.

On the other hand, participant experiences that are represented as a subset of the data should be considered as part of the variation within the data and may be generalizable, from a qualitative standpoint. For example, fifteen participants in total admitted to or described

[3] Katz (1997, p. 415) refers to these underlying meaning structures in social life as "communal realities."

engaging in some form of illegal social engineering, and descriptions of some illegal social engineering experiences are explored in the first research question, "*What are the experiential dimensions of engaging in social engineering?"* The illegal social engineering experiences described by participants provides variation for the context in which the social engineering took place, while still elucidating the same thematic meaning structure of the experience of social engineering. Thus, while the meanings described by the themes are likely to be reflective of broader social engineering experiences, the limitation of these qualitative results is that no declarations can be made generalizing the proportion of instances, or themes, in the results to the general population (Weiss, 1995).

Data Gathering

The 54 interviews that occurred with social engineers, security auditors, and other IT professionals ranged from 43 minutes to four hours and four minutes in length. Utilizing interviews allowed participants to describe in-depth both their experiences and their understanding of the topics under investigation (Rubin & Rubin, 2005). The process of using semi-structured interviews to explore a research topic begins with the creation of an interview guide, or schedule (Berg & Lune, 2012; Weiss 1995). This guide generally consists of main questions, which cover the topics related to the research questions the researcher would like to examine (Rubin & Rubin 2005). In this project, three interview guides were created: a guide for social engineers, a guide for Information Security Professionals, and a guide for security auditors who use social engineering in their professional work. Using the interview guide allowed all participants to respond to respond to the same questions, however, follow-up questions and probes were also used. The use of follow-up questions encourages participants to have depth and detail in their responses, as well as to explore interesting ideas that the participants might suggest

(Rubin & Rubin 2005). The particular qualitative data that were analyzed were the deidentified transcripts from audio recordings of the semi-structured interviews.

Semi-structured interviews were the most appropriate data collection technique for analyzing the research questions in this dissertation. Each research question is concerned with a certain area of knowledge or experience, necessitating the use of a set of standardized questions to elicit thoughts and narratives from the participants (Berg & Lune, 2012). As participants may have a wide range of experiences and beliefs, the semi-structured interview is also most appropriate for allowing each participant the flexibility to discuss the areas of relevance that may be of particular significance for themselves. The ability of the semi-structured interview to accommodate spontaneous discussions by the participants is noted by Berg and Lune (2012) to result in "a much more textured set of accounts from participants" (p. 114). This form of interviewing was thus be used to gather rich qualitative data from social engineers and security auditors.

Data Protection

Ethical considerations necessitate that all data derived from human-subjects research be protected to prevent harm from occurring to participants who must willingly and freely consent to participate in research (Berg & Lune, 2012; Esterberg, 2002). As all social engineers and IT professionals who were recruited for this project are adults and not from vulnerable populations, the process of these participants participating involves acquiring informed consent from the participants prior to the commencement of an interview. Informed consent entails ensuring that participants know that they are participating in research, that they understand the scope and potential risks of the study, and that they choose of their own volition to participate, and that they may withdraw from the research at any point (Berg & Lune 2012; Corbin & Strauss, 2015).

Typically, informed consent is documented by requiring that participants read and sign an informed consent form (Berg & Lune, p. 92). For this research project, however, the requirement to sign the informed consent forms was waived, in order to reduce the amount of information linking participants to the project.

All interviews and participant information collected for this project were protected to maintain participant confidentiality. To maintain participant confidentiality, all identifying information (e.g. named locations, business names, personal names) were removed from interview transcriptions. The participants were also assigned pseudonyms to replace potentially identifying information. In publications, any experiences reported by participants that are unique enough to be potentially identifying will be only used for analysis or will be summarized to be sufficiently general to remove identifying characteristics. Interviews are conducted through encrypted voice over internet protocol (VoIP) programs, or in-person. All data is stored either on hardware encrypted external media or secured in locked offices and filing cabinets. All interview audio recordings will be destroyed at the conclusion of the project.

Analytical Approach

For each research question, the preparation for data analysis entailed entering the interview transcriptions into Atlas.ti Version 9.1.2 for data management. The transcribed text was then qualitatively analyzed through a process of coding the portions of the transcriptions that are relevant for each research question. As there are three separate research questions that are investigated within this dissertation, there were three separate analyses that occur: one for each research question. The analytical approach that will be used to investigate the research questions is grounded theory.

Grounded Theory

Grounded theory was originally developed as an analytical approach to qualitative data by Glaser and Strauss, (1967) and provides as systematic, but flexible, method of analyzing a wide range of qualitative data. This analytical approach is focused on the development of theory construction, rather than describing or applying extant theories to qualitative data (Charmaz, 2014). Theory, in this analytical approach, refers to "a set of well-developed categories (themes, concepts) that are systematically developed in terms of their properties and dimensions and interrelated through statements of relationship to form a theoretical framework that explains something about a phenomenon" (Corbin & Strauss, 2015, p 62). The ability of this method to aid the researcher in generating theoretical frameworks through an interpretive analysis, while remaining adaptable makes it a useful analytical approach for this dissertation. A grounded theory analysis will therefore be used to explore the research questions: "*What are the experiential dimensions of engaging in social engineering?"* "*How do social engineers attempt to maintain deceptions while engaging in social engineering?*" "*How does deception detection occur across social engineering interactions?"*

Grounded theory employs an iterative coding approach for the purpose of analyzing qualitative date to discover themes and construct theories that emerge from the data in the process of analysis (Lindlof & Taylor, 2002). The researcher inductively crafts theoretically grounded explanations of social phenomena through a multi-level systematic analysis of the data. In this capacity, "data and theorizing are intertwined. Obtaining rich data provides a solid foundation for developing "robust theories" (Charmaz, 2002, p. 667). The process involves the transformation of data into concepts which are them summarized into broader analytic categories. As the process unfolds, patterns begin to emerge.

Corbin and Strauss (1990) advocate for three stages of the process of data analysis—*open coding, axial coding,* and *selective coding*. Open coding involves comparisons between units of data and the assignment of conceptual labels. This initial coding process may be aided through the use of 'sensitizing concepts.' According to Charmaz (2014), sensitizing concepts "give you starting points for initiating your analysis, but do not determine its content" (p. 117). These codes are provisional, and may be changed as the researcher continues the process of reading and rereading the data (Charmaz, 2014). This process of open coding may be conducted in a variety of ways, but in this case will occur through line-by-line coding. This process entails first reading through all interviews and labeling 'chunks' of meaning with brief descriptive terms (Wertz, et al., 2011). These chunks may be words, phrases, entire sentences, or several sentences.

Axial coding means that the concepts that begin to emerge from clusters of open codes are compared to each other and categories are developed to organize the concepts (Charmaz, 2014). This step of the coding processes allows the relationships between concepts to be explored, as concepts can be grouped and regrouped together as the researcher explores the potential connections between categories (Charmaz, 2014). The result of the process of axial coding is that previously separate categories are brought together under a new conceptual category (Lindlof & Taylor, 2019).

The process of comparing each level of analysis (data, concepts, and categories), refining these levels, and developing one or more "core" categories to organize to totality of the data is *selective* coding. In this last step, the "core category represents the central phenomenon of the study" (Corbin & Strauss, 1990, p. 14). It is at this stage of analysis that explanations for the patterns throughout the research are unified through a common explanatory mechanism(s).

Editorial and Typographical Conventions

Throughout the next three chapters of the dissertation there are two editorial and typographical choices that are consistently employed in the text. Each of these considerations regards how participant voice and identity is incorporated into the analysis and results of the three research questions explored in this dissertation. For the clarity of the reader, they are explicated as follows:

1. When possible, illustrative quotes have been taken from participant interview transcripts to reinforce the analytical themes within the results. In many cases, these quotes have been edited for length. In each case where words were removed from a sentence or paragraph within the quote, an ellipsis has been inserted into the quote to indicate that the participant transcript has been modified in this manner. When the quoted portion of the transcript begins or ends mid-sentence, the quote will begin or end with an ellipsis to indicate this abridgement of the participant's speech. This typographical choice was made to demonstrate where authorial modification of a participant's words had occurred. Every effort was made to preserve the meaning and intent of the participants throughout the editing process.
2. To preserve participant anonymity, all participant names used throughout this dissertation are pseudonyms. These pseudonyms were assigned at the time of the interview, either by the researcher conducting the interview or chosen by the participant themselves. As each interview corresponds with an individual pseudonym, the same participant would be referred to across all three analyses in this dissertation by the same pseudonym. The pseudonyms are the only feature of

participant identity that has been altered. References to participant gender, occupation, or any other individual characteristics are based on information provided by the participant during the interviews.

Chapter 4 - Analysis: Felt Experience of Social Engineering

Three intertwining dimensions emerged in this analysis as constitutive of the experience of social engineering. Engaging in social engineering is revealed as a felt experience, and participants often reported feeling intense emotions as they entered these interactions. The fundamentally interactional dimensions of the experience also become apparent, as social engineers are often oriented towards both themselves and the other who is being targeted in the interaction. The experience of uncertainty permeates the experience of social engineering interactions, and while there is often an intentional attempt to mitigate this uncertainty, many social engineers also find satisfaction and enjoyment in the unpredictability of the experience.

Felt Experience

For social engineers, the emotions experienced in social engineering undergo transformation across the course of a social engineering engagement. Shifts in emotion were frequently described by participants as they approached and initiated social engineering interactions, once they were actively engaged in such interactions, and at the resolution of the social engineering attempts.

Most participants described a sense of trepidation that preceded initiating a social engineering encounter. The experience of apprehension felt by the social engineers was typically described as a sense of anxiety, nervousness, or fear. As Edward, an experienced social engineer, stated, "I've always, always freak out, always get nervous before I give a talk, before I go on stage, before I go do an engagement. There's always that like, 'Oh, I'm gonna fail. It's gonna be miserable.'" While this initial nervousness shifted into other emotional states for some participants, other social engineers experienced trepidation throughout the entirety of these interactions.

The apprehensiveness experienced by participants that ran through social engineering experiences was expressed as emerging from two distinct aspects of the engagement. Some social engineers described experiencing great anxiety, fear, or terror due to the potential consequences of failing to convince their social engineering targets. The trepidation evoked by this concern is most clearly apparent in the narratives of social engineers who found themselves in unplanned and involuntary interactions with authority figures, such as law enforcement. Bernard described using social engineering in this context by saying:

> …I guess, the thing with the police when I was in the interrogation room, I guess that was probably my first getting out of trouble with social engineering… And I still, you know, like that was pure, I was scared absolutely shitless, you know…I mean, at the time, I think I was mostly just scared and hoping to find a way out of it 'cause I knew I had done a lot of illegal things at that point in time

Fear of consequences was not the only source of apprehension, as social engineers engaged in legitimate, legal social engineering also described experiencing nervousness and anxiety, even while explicitly stating that their social engineering interactions posed no risk for themselves. Anna, a security auditor, highlights this discrepancy by saying:

> I think that the thing that's really interesting about risk is that for me, personally, there is no risk because all of my activities are legal, and sanctioned, and requested by client, right?...What's interesting, though, is that a lot of folks that are new into this field, feel like there's a risk of getting caught, you know, that's a big fear, is that I'm gonna make phishing call and someone's gonna bust me on this.

Therefore, there is also a more essential aspect of anxiety that lies within the interaction itself. The social engineer experiences trepidation at the thought of failing to convince the target that a fabricated reality presented by the social engineer is, in fact, the truth, regardless of the absence of consequences regarding this failure.

While social engineering interactions may be experienced as unpleasantly nerve-racking or terrifying, the uncertainty and apprehension experienced by the social engineer is often described as fun, exciting, enjoyable, and as a thrilling adrenaline rush. Edna described this experience and said, “It’s definitely, I think, an adrenaline rush, well, when it’s successful. Just a huge, you know, I associate it to, I’ve done baseline jumping once…that feeling, that rush, it just, I don’t know, it feels great.” This excitement and thrilling aspect of social engineering was often characterized as a significant motivation for engaging in the experience.

Some social engineers characterized their experience of social engineering primarily of one of enjoyable excitement. More frequently, however, participants described feeling an initial apprehension while beginning a social engineering interaction, which transformed into feelings of excitement and exhilaration as the interaction progressed. Lucy’s statement reflects a typical description of this type of experience: “It’s really nerve-racking to actually walk on to a site but all of the adrenaline that’s on the back end of it is fantastic. And I like that.” This shift of emotions was described by several participants as analogous to the experience of riding a rollercoaster. One such rollercoaster experience was described by Daniel:

So you’re nervous as heck and then you send the email and you can’t control when someone looks at it, so you’re sitting there staring at a screen with a black box on it for hours…and all of a sudden…you’re like, “Yes, we’re in!” And, you know, it was like riding a rollercoaster and that fear when you’re going up that first hill but then the exhilaration when you’re flying down the next hill is, that’s what it felt like.

Descriptions of thrill and excitement, like those of apprehension, may be experienced with regards to separate dimensions of the engagement. Some social engineers described gaining access to locations as thrilling, as well satisfying a curiosity or sense of exploration. Victor expresses this sentiment by saying:

> I've always wondered if I could rob a bank and get away with it, but it's illegal. So now being in a career where I could, I'll wonder if I could get in and install my backdoors, or I wonder if I could get into their wire transfer system? …And it's, it's really exciting.

Other social engineers describe the experiences of gaining access to restricted areas via technological means as distinct from the experience of social engineering. Describing social engineering as more fun that alternative ways of gaining access, Edward said, "…I can do some network based attacks and hacking but where's the fun in that?… I'm literally doing this my way because it's just more fun…I've never broken into a shoe store in Cleveland - it's not interesting."

This excitement expressed by some social engineers emerges from a component of social engineering interactions, but is not particular to social engineering interactions, as the thrill of accessing restricted domains does not necessitate a social interaction take place. For some social engineers, there is also sense of thrill imbedded within the social engineering interaction itself. Walter describes the connection between this thrill and fear and says:

> I'll say that it's the risk of being identified, of being exposed that builds the adrenaline that drives me to do it….what else would create the adrenaline if not for fear and what would be creating the fear if not the exposure of my real identity?

Notably, this these feelings of risk described by Walter occurred during professional security audits that he had been hired to perform, and so do not express the potential risk of legal consequences stemming from the revelation of his true identity. Instead, thrill in this context coalesces around a felt concern with being able to convince a target to accept the engineer's framing of reality as valid, while accompanied by the fear of the target resisting these attempts. Ida also described this aspect of the social engineering experience as thrilling and said:

Successfully deceiving someone, it might sound kind of psychopathic. It's, it's a thrill. It's, it's very exciting to be able to get away with a lie concocted and convince somebody that you're someone you're not, or not even be questioned about who you are, or have to explain your presence.

As a social engineering interaction draws to a close, social engineers describe their feelings as being shaped by their perceptions of the success or failure the interaction. At a perceived success, the sense of excitement may be accentuated or adjust into a feeling of victory. Claire expresses these feelings in her description of her feeling of success in one of her social engineering engagements, and said:

> I mean, you know, some Mission Impossible theme music plays in the back of your head and it's exciting because you tricked these people and you were successful and because of that, you get to be places that you're not supposed to be.

In contrast to the experience of social engineering success, the perception of failing at a social engineering interaction transforms an exciting interaction into an experience of frustration. Jeremiah described this frustration as related to his perception that social engineering ought to be relatively easy to accomplish and said:

If it's going good, it's exciting, especially when you, you know, you gain their trust and you, you know, you get in, but it also can be extremely frustrating because, as I've said, usually social engineering's the easy way in, and so when it's not working, it's extremely frustrating because this is supposed to be the easy way.

Other social engineers describe the resolution of a social engineering interaction as being felt as relief, as they can then withdraw from an anxiety-provoking situation. The initial feelings upon the resolution of a social engineering interaction may further resolve into a sense of satisfaction on the part of the social engineer, or a sense of guilt. Marilyn described her experience at the close of a social engineering interactions by saying:

> I always get nervous but it's also kind of cool when you're actually, when it's working, it's very thrilling. And then for me, depending on the experience that I had, it can either still be exciting or it can kind of turn into, I have a little bit of like guilt and remorse for, for, you know, getting people to give me information.

Social engineers also tended to describe feelings of guilt if they perceive that their targets have negative emotions about the interaction or if the targets experience negative consequences, such as job loss, as the result of the interaction.

Not all social engineering experiences are experiences of intense emotions, or motivated by enjoyment of the process of social engineering. Some social engineers described perceiving social engineering as relatively boring or mundane, especially by experienced social engineers. David describes feeling this way about engaging in social engineering using phone calls and says, "I mean, it feels like, 'Okay, here's another one.' Like this mundane, routine thing… I mean, for me, it's not exciting at all." August, an experienced social engineer, expressed becoming desensitized or numbed to social engineering. He said:

There are definitely levels of repetition that occur so, you know, sometimes you just kind of numb to it, I guess. With that being said, I mean, you know, it's always, it is still fun but, yeah, sometimes, you know, when you've done something so many times and you know it's gonna work, I mean, you know, you just kind of get numb to it.

August attributes the reduced emotional intensity he feels in social engineer as related to knowing that his attempts at social engineering will be successful, and this is reflected in the narratives of other social engineers who felt secure and confident in their abilities and also express some amount of boredom in social engineering interactions.

Interactional dimensions

The intrinsically relational character of social engineering substantially shapes the experience of engaging in social engineering. The interactional dimensions that are influential to the experience of social engineers emerge from the understandings that social engineers have of the targets of social engineering, as well as the understandings that social engineers have of themselves. These understandings influence both the character and the intensity of the emotions felt during social engineering.

Relational distance

The channels of communication used by social engineers shade the entirety of the interactional milieu in which social engineering occurs. Some forms of communication are experienced as bringing the other into relational closeness with the social engineer, while other communication methods produce a wider social distance between the social engineer and the target. Interactions that occurred across greater relational distances, such as email, were often characterized as less emotionally intense, and more predictable, than those involving greater relational closeness to the target. Although social engineering can occur across many communication mediums, the participants specifically discussed only email, phone calls, and face-to-face interactions as forms of communication that they had used for these purposes.

Every social engineer who described different methods used for communication expressed that email was the most indirect, impersonal, and most socially removed form of communication. Lucy expressed a perspective commonly shared by the other participants regarding the distinction between the various channels of communication by saying, “Email’s very impersonal. Phone calls are more, much more personal, and then in-person is about as personal as it gets 'cause you're right there talking to people." In social engineering interactions over email, the target is focused on primarily before the interaction is initiated. Anna described this distinction that occurs in phishing, and stated:

The phishing, I think, is different because people have a little bit of time, you know, they have a little bit of space to kind of think about what they want to do, and that's when the ability to pull in pieces of information or appeal to them emotionally in some way because important.

As Anna elucidated, the focus of the social engineer using email is directed towards discovering target attributes that might increase susceptibility to responding to the message crafted by the social engineer.

The breadth of social distance over email and the perceived impersonal characteristics of this form of communication created a sense of disconnection between the social engineers and their targets. The disconnection that occurs across the social distance of email communication is expressed by Gerald, who discussed a social engineering engagement that he conducted using phishing. In this engagement, he discovered that the company he was phishing had a relationship with a nonprofit organization, and so he crafted a phishing email that purported to be from this nonprofit and sent it out to the employees of this organization. He described his perspective and stated:

> And it made me feel dirty because who isn't gonna click on a…link around the holidays? Everybody's going to, especially if that's part of the company culture. You know, and it, thankfully, it was a phishing email so I wasn't, you know, face-to-face with people 'cause, yeah, it made me feel dirty.

For Gerald, the lack of personal connection to these targets allowed him to engage in a pretext which he found to be unpleasant and might not have used in a face-to-face setting. This sense of disconnection is felt as a more muted emotional experience than social engineering through more direct communication channels. Marilyn described her feeling about the different communication channels in saying:

> Like I always get the nerves and, you know, still kind of that excitement and then depending on if it, if it was just emails, not so much like the guilt or remorse, but if I did a lot of like actually human interactions, sometimes I do have a little bit more of that like, 'Oh, like we had a really great conversation but I was a bad guy and you didn't know.'

The language used by Marilyn in this description is revelatory of her perspective, as she specifies emails as distinct from "actually human interactions," as though the use of emails does not constitute an interaction with another human being.

Social engineering interactions that occur over the phone were characterized by social engineers as more personal than email and these interactions were often described as experienced with apprehension and excitement. Eustace highlights this experience:

> When you do a vishing, which is voice phishing email engagement, you're calling somebody, you're, the first time you're doin' that phone call, you're nervous, and I don't care who it is, everybody's nervous for that very first part of the phone call.

While often considered a direct form of communication, phone calls were perceived by some participants as more socially distant from targets and impersonal than face-to-face interactions. This was the perception John expressed:

> On the phone calls or an email, I don't really care, right? That's easy, you don't have to interact with a human being directly, necessarily, in-person. There's a lot of anonymity that comes, like a phone call, you know, you could call somebody up and say anything you want and what are they gonna do to you, right?

The ease of disengaging from the interaction by hanging up and the fact that the target cannot be directly seen and cannot observe the physical aspects of the social engineer contribute to the experience of social distance in these interactions.

Just as every social engineer agreed regarding the relational distance created by email, all participants also agreed that face-to-face interactions were the most personal and created the least perceptual distance. Clarence described the intricacies that he considered in face-to-face social engineering in particular, and stated:

> A huge part of it is body language, reading facial expressions on somebody. Just, just kind of gettin', getting that vibe from somebody about should I keep pressing a little bit more, should I turn my body just so, should I, you know, lower my tone, speed up my talking, match, you know, if they're, you know, with their arms closed or a little bit closed off, I'll try to mirror that a little bit.

The relational closeness of this interactions was experienced by the social engineers in their inability to disengage from the target and the perceptions of managing presentation of self to the target with regards to physical presence, rather than this presentation being restricted to written tones or verbal intonations.

The relational closeness experienced in these face-to-face interactions is associated with the intensity of the emotions experienced by the social engineers, as well as the challenge of engaging in social engineering across this communication medium. Walter describes the rush of face-to-face interactions by saying:

> So the challenge to do it in person where I'm face-to-face, you know, that's the adrenaline rush where, you know, I'm now looking at you in the face and I'm telling you that I'm somebody that I'm not, and I'm asking you to give me access to your bank. So that's, that, to me that's where the reward is, that's the draw for me is the adrenaline.

While social engineers like Walter highlighted the appeal of the intensity of face-to-face social engineering, several other social engineers saw this intensity as a reason to avoid social engineering in this context.

Framing targets

While social distance shapes experiences of relational closeness between the social engineers and their targets, the meaning that social engineers give to their targets transforms the experience of engaging in social engineering. For social engineers, the process of social engineering entails an attempt to convince the target of social engineering that intentionally falsified information is true. These situations are ones of knowledge asymmetry, as the social engineer knows from the start that the interactions are not as they seem, while the target lacks this foreknowledge and must determine the nature of the interaction as the interaction occurs. In this context, some social engineers construct their targets as opponents in a strategic game who are to be defeated, while other social engineers understand their targets as individuals made vulnerable by these situations and who should be helped.

Social engineers often described targets as being opponents and framed their targets as opponents in a strategic game or battle. Some social engineers offered a generalized description of this analogy, such as the statement by Mark that “You know, you get a bit of a rush off of it, I think. You know, it’s kind of a game at some level, so it’s a fun game to play.” Harold highlights the role of the target in his analogy of a chess game, saying:

> …Going back to the chess game analogy, you want to play somebody that’s, if you really want to know if you’re any good at chess, you got to play somebody who’s pretty good, and there’s a little bit of that game going on, I think, in any social engineer...How can I find an adversary that will help me determine how good I am?

Perceiving of targets as adversaries shades the entirety of the experience of social engineering; turning the interaction into a hunt, and success into a victorious win.

Feeling victorious in the wake of engaging in social engineering is associated with the perceived challenge posed by the experience. This perspective is expressed by Clarence's statement that "Just like with anything, it's, it's the thrill of the hunt. It's the challenge of it... I never really thought about it until just now but being able to deal with an adversary." Feelings of thrill and victory manifest in interactions where the social engineer understands themselves has having fairly defeated a worthy opponent, in contrast to an opponent with perceived weaknesses. Harold expresses this sentiment in saying, "I mean, there, it's great to win but if, only if you have a worthy adversary." The perceived extent to which the interaction is challenging to the social engineer is thereby linked to the satisfaction derived from the success of the interaction.

Social engineers may also understand targets in social engineering interactions as vulnerable individuals who need assistance and education to reduce their susceptibility to social engineering. The experience of social engineering for social engineers who understand their targets in this manner can be analogous to a teacher administering a test for educational purposes, rather than the strategic playing of a game against an opponent. Zeb described taking this stance in his security audits that involved social engineering and said: 'I'll usually reveal myself to the person that I was most focused on or whoever I was able to leverage the most, to let them know what happened and try to educate them on where they went wrong and what they can do better next time.'

Some social engineers with this perspective of targets emphasize that the knowledge asymmetry intrinsic to social engineering interactions makes anyone targeted in such an interaction vulnerable to social engineering. Daniel expressed such a view of targets and stated that, "They're human, and as long as you're human, I can get you to fall for something, I just need to find what the right emotional trigger is and I can get you to fall for it." Feelings of sympathy for the target are may emerge from these perceptions of target vulnerability. Other social engineers construct targets as vulnerable, but understand some targets as perilously vulnerable and in need of discipline rather than assistance.

Feeling of satisfaction may be experienced by social engineers who construct targets as vulnerable people in need of assistance when the targets detect their attempts and react appropriately. Muriel described feeling this way about individuals targeted by her during security audits and said:

> …You're trying to give people the opportunity to stop you. So in a way getting caught isn't even a bad thing, it's a good thing. So you're trying to say "We're there, you just have to stop me." That's awesome, I mean, you've got good security in place.

These feelings of satisfaction for the success of the target may at the same time be accompanied by feelings of frustration stemming from the perceived failure of success.

These two constructions of what it means to be a target of social engineering may be simultaneously held while engaging in social engineering. Lucy described the holding these conflicting orientations during her work as a security auditor, stating:

> It's really hard for me to, when I'm feeling very, like gleeful and awesome about how I've, you know, broken stuff or gotten to places I'm not supposed to get to. But then to talk about that in an appropriate way, because to a client, no, it's not awesome, it's not exhilarating or awesome for them, it's concerning. And making that, trying to do that rapid switch is very hard for me.

As demonstrated by Lucy, maintaining both these perspectives of targets results in cognitive dissonance, as the social engineer mentally grapples with the satisfaction and thrill of overcoming a target perceived as adversarial, while at the same time maintaining sympathetic evaluations of the target as vulnerable.

All social interactions necessitate some degree of awareness and attention of the others in the interaction. When engaging in social engineering, this focus on the other is amplified, as social engineers focus intently on the reactions and responses of their targets. Social engineers are particularly concerned with preventing targets from becoming suspicious and mitigating the targets, as the engineers attempt to grasp the target's perception of the situation, and to see interaction as the target understands it.

This attention that social engineers have about target perspective is primarily focused on ascertaining and averting misgivings targets may have about the interaction. Social engineers often described experiencing anxiety at the concern that the target of social engineering might become suspicious. Claire experiences this in a social engineering engagement where her pretext involved emailing the company a pretext about being a consultant who needed to do an inspection and then attempting to compromise security at the company's location. She describes her experience and says:

> So this was my first time by myself and I was pretty darn nervous about it. I walked in and the branch manager walks out of her office before I even say anything to the tellers and names me by name and I'm like, "Oh, I'm screwed." And she was like, "Oh yeah, I just got an email that you were gonna be here. It's so nice to meet you. Blah-blah-blah. What do you need to see?"

Even in the absence of circumstances that would prompt a target to become suspicious, social engineers often experience thoughts that they will be or have been found out by their targets. Bernard expressed similar feelings in a social engineering engagement that he had conducted and said:

> And I just walked in and they had little badges, and they had a fancy elevator with digital screens, the whole shebam and I'm like, "I'm gonna get busted." And nobody even

> looked at me twice. It was, it was ridiculously easy. I was, of course, sweatin' bullets, nervous, sure I was gonna get caught, you know?

These experiences are characterized by nervousness about the potential suspicion of the targets in social engineering and in the absence of target suspicion, social engineers often describe experiencing surprise or shock at the lack of such suspicion.

Social roles and aspects of social identity are used by social engineers as ways of understanding what the perspective of a target might be. Arlo described focusing on the social roles entailed by a target's job, and often try to understand the target's perspective based on these:

> It all depends on who you're trying to talk to, even at the same company, you try and talk to five different people - a security guard, a receptionist, an employee, they're all gonna require different pretext and different challenges and a different background, all depending on who you're trying to be with those people.

Gender and age are also aspects of identity that social engineers may use to try to understand how a target perceives a situation. Marilyn offers a perceptive using these social identity attributes when she says, "…Older women in their fifties just kind of have this way of like, 'No. That's not how we do things here.' Like they're just pretty quick at shutting people down."

Social engineers also scrutinize the emotive expressions of potential targets, often choosing to interact with people who they perceive to be happy and outgoing, as these individuals are thought to be more likely to perceive interactions without mistrust. The same empathetic orientation to the way the target feels that allows social engineers to evaluate target suspicion may run through the entirety of the social engineer's perception of the target, even in the absence of the functional end of mitigating target suspicion. A notable example of this was described by Zeke who used an email offering free iphones to phish employees during a security audit. He said:

> …One of the ladies that fell for it had emailed me directly because, you know, we had a fake email address and emailed the fake email address and said, "You know, I've worked at this company for 25 years and it is one of the greatest companies that I ever worked for. My daughter, you know, is in the hospital with cancer and I couldn't afford, you know, I couldn't afford, you know, iphone, this is gonna be a great Christmas gift."…So I actually bought an iphone and I sent it to her, you know, like I'm not gonna mess with that type of stuff, you know? But, you know, it can have a major impact on how you treat people and the certain things that you do and you just have to be cognizant of that.

In this case, Zeke's phishing attempt was successful because he was able to see from the perspective of his targets what email content might appeal to them and motivate them to give up their credentials. At the same time, however, Zeke empathetically understood the perspective of the lady whom he had successfully targeted, and was motivated by this understanding to assist her despite the financial cost to himself.

More commonly, this extension of empathy for the target is expressed by many social engineers who report experiencing feeling concern at the thought that the target might feel bad or suffer from negative consequences because of the social engineering interaction. This concern about the emotional states of targets may be felt as guilt, which social engineers sometimes mitigate with justifications about the benefits of their actions. Social engineers may also alter future social engineering situations to reduce the perceived negative experiences of future targets.

Understandings of self

Just as the understandings of others are dimensions of interaction that shape the experience of social engineering, the understandings that social engineers have of themselves likewise do the same. There are two aspects of understanding self that are of particular salience in the experience of social engineering: self-assurance and perceptions of skillfulness. Skillfulness refers to the proficiency that social engineers possess in areas relevant to social engineering, while self-assurance refers to the self-concept that social engineers has of themselves as individuals who could successfully accomplish their own goals.

Skillfulness.

The ability to effectively implement relevant skills impacts the experience that social engineers have when engaging in social engineering. Three skills emerged from the analysis as of particular significance to the social engineers in social engineering interactions: emotion management, pretext management, and conversational ability.

Social engineers described two approaches for managing their emotions. First, some social engineers used behavioral strategies to reduce anxiety before or after social engineering interactions. Robert describes specific techniques he uses to mitigate negative feelings while engaging in social engineering and said:

> I can make two or three calls in succession depending on how the call goes. Because, you know, of course the greater the risk or the, you know, the closer to the edge of getting caught that I get and if I'm able to kind of bring myself back out of it, it causes more of that response, so some calls get kind of intense and after those calls, I literally have to get up and walk around and kind of shake my hands a little bit and just, you know, maybe walk outside or somethin'.

In addition to using methods to reduce the intensity of emotions, social engineers also focused on having control over their emotional expressions. Ida emphasized the importance of controlling emotional expressions and said:

> If your story is I'm just here for another day of work and I'm bored and I'm, you know ho-hum, you know, then you have to be able to pull that off convincingly and not let the

> adrenaline that's going through your system at that moment change your demeanor because it's hard, it's hard to put something different on your face or in your voice than what's really going on internally.

While the social engineer might experience intense emotions in these situations, their concerns centered around not expressing these emotions to avoid creating suspicions in the target.

The process of crafting a pretext through research and information gathering was itself part of the experience of social engineering, and some social engineers expressed enjoyment and satisfaction in this process. Lucy was one of the social engineers who expressed this by saying, "I love doing the research. I like coming up with a good pretext." Other social engineers, on the other hand, found researching pretexts as boring or unexciting, and some experienced frustration in this process.

Pretext management was used by social engineers to not only increase their chances of success, but also to either heighten the excitement of social engineering or to reduce anxiety associated with social engineering interactions. Zeb provides an example of using pretexts to avoid boredom in this manner, and says:

> One of my dreams is to do a social engineering engagement during the holiday season, say Easter or Christmas, so I can enter the building dressed in character, as Santa Clause or the Easter Bunny…Like I don't like to always say, "Oh, I'm with IT and I'm supposed to do this thing." …That one does bore me after a while. I don't like to repeat the things. I like to try the different things.

Along with Zeb's use new pretexts for engagements and choosing pretexts that involved unconventional and amusing behavior, pretexts can also be used to make social engineering interactions more exciting through engaging in minimal information gathering before attempting a social engineering engagement.

Conversely, social engineers also used pretexts to alleviate anxiety experienced in social engineering interactions. Pretexts used for this purpose were often extensively thought through and all aspects were memorized by the social engineer prior to the social engineering attempt. Patrick described this type of approach to pretexts before using them in social engineering calls. He said:

> And also, yeah, and also one thing that I try and do is I try to build or research my persona beyond what's likely to come up on the call…And I, that gives me the comfort level where I think I can be that persona on the phone without having, and I can stay in character more easily.

Often social engineers seeking to mitigate anxiety would repeatedly use the same pretext because they were familiar with it and felt confident in implementing it.

Pretext management also frequently involved social engineers employing aspects their social identity in crafting a pretext. Often this would involve the social engineer drawing on past work experience or attributes such as age or gender in the creation of a pretext. Edna described this form of pretext management in relation to her perceptions on gender roles and said:

I'm a girl. I don't make sense in IT. And I don't care if that's, you know, PC or not. That's what people think. So I think being able to kind of step back and look at the bigger picture, how people are gonna see you and how people are gonna even really relate to you, just make, so a lot of times when I do these engagements, I try not to be from IT... So I play more of an auditor role or something that makes sense for the company.

Conversational ability was also frequently discussed by social engineers as a skill that shaped their experiences of engaging in social engineering. One relevant aspect of conversational ability regarded the basic ability to hold a conversation in a social engineering setting without making the target feel uncomfortable. Anna expressed this by saying, "And, one of the keys to being able to social engineer someone is to be able to make someone comfortable, you know, to be able to make someone feel like you're friendly and interested in conversation." Feelings of nervousness often revolved around concerns with not knowing what to say in social engineering interactions, how to disengage smoothly from these interactions, and how to interact without being perceived by the target as threatening.

For social engineers who felt they had mastery over the former aspects of conversations, conversational ability provided a way of building rapport and gaining control over the interaction. Zeke offers describes a situation where he and a partner encountered a security guard while attempting to break into a building and used their conversational abilities to gain control over the situation and alleviate the security guard's suspicion:

> We get into the building and, you know, we're walkin' about the building and we get busted by the security guard…You know, like, I mean, we look like burglars. Like if you took a picture of us, you could use that as like photo stock, you know, or for burglar pictures, right?...And, so the security guard is like all paranoid, he's like, "Who are you guys? What are you doing here, you know, late at night?" This is like two o'clock in the morning. And the guy next to me, you know, that I'm with is like, "Hey man, you know, it's, we're in IT, we're just workin' late, the servers crashed. Got everything back up. I'm sorry if your internet was slow, you know, we fixed all that." He's like, "Oh yeah, like I noticed the internet was a little slower earlier." He was like, "Alright. Cool, man." He goes, "Let me know when you get in here. I didn't even see you come in." I'm like, "Yeah, cool man. It's fine," we walk out, you know? And, you know, that conversation piece of it was so important because you can literally get yourself out of any situation you want to.

Social engineers also often focused on the emotions and attitudes they expressed in conversations as important to convincing the targets of their social engineering interaction.

Self-assurance.

In addition to skillfulness, confidence in self is often characterized by social engineers as crucial for their own success. Some social engineers describe already having confidence in themselves during their initial forays into social engineering and often attributed this confidence to personality traits. For many other social engineers, however, their first attempts at social engineering were fraught with anxiety and a lack of self-assurance. Claire shared her experience of entering into social engineering initially and said:

> My first, the first time I did physical social engineering and trying to get into a facility, I was a complete mess. I was nervous, I stammered, you know, like puked afterwards - it was terrible. I was not convincing at all, by the way…after I got past that, the second time... I got a lot more confident and then afterwards, I, because of that confidence, I was able to get more creative and more, you know, understanding of what works and what doesn't, how I can do all of this.

This lack of confidence is described not only as an unpleasant emotional state, but also as a substantial impediment to success in social engineering. Dorian highlights the importance of confidence in relation to success by saying:

> And, I think it comes down to if you're a social engineer, you have that confidence. Even if it's just as simply as just walking somewhere and then having a normal conversation with somebody… I think that confidence and that ability to just kind of, in your mind, say, "Okay. I'm supposed to be here. I'm supposed to be having this conversation. I'm supposed to be talking to this person," is a big, huge, huge piece of it.

Gaining experience in social engineering through practice and repeated attempts is often characterized by the social engineers as one of the key ways in which confidence can be gained. Malcolm described this perspective in the context of experience he had gained through experience with social engineering:

> You know… a lot of people get a lot of social anxiety right out of the gates and, you know, the more and more you do it, the more and more it desensitizes you to, to certain things, or at least to the initial approach, and you also just get this confidence and

> boldness behind the things that you do, so, you know, you end up doing way crazier things over time and executing them with a lot more confidence than when you first started.

Like Malcolm, other social engineers described gaining experience through repetition, becoming more confident, and having reduced apprehension in their experiences of social engineering interactions. Some social engineers attempt to build both their confidence and abilities through practicing interactions that are experientially similar to social engineering interactions. Techniques to achieve these goals range from talking strangers and attempting to acquire particular facts from them, to enrolling in improv classes.

Discussion

The purpose of the present study was to investigate narratives of social engineering experiences in an effort to reach a deeper understanding of the meanings and motivations held by social engineers. The dimensions of the felt experience of social engineering is fundamentally interactional for the social engineer, as both awareness of self and awareness of the others who are targeted by social engineering pervades the experiential foreground of these encounters. The intensity and quality of the emotions brought forth in social engineering interactions denotes the contours of meaning that the social engineer brings to these interactions.

The common emotional structure of a social engineering experience, as well as variations in this structure, are particularly revelatory of the meanings that constitute engaging in social engineering.

Although the emotional intensity and prevalence of emotions variety between both participants and individual engagements, typical descriptions of social engineering linked the emotions of anxiety and excitement. Often a social engineering encounter would be approached with trepidation, even to the point of overwhelming anxiety, which at a certain stage of interaction would transform into a positive affective experience, such as a sense of thrill, rush, or exhilaration.

To some extent, the felt trepidation in social engineering manifests relatively apparent meanings of the experience for the social engineer. Social engineering engagements may create the danger of potential conflict, and perhaps even a perceived risk of bodily harm if the location the social engineer attempts to compromise has armed security guards. The meaning of anxiety in social engineering does not simply demonstrate a concern with potential harm, however, as social engineers describe experiences of anxiety when engaging in legally authorized social engineering interactions, which may even occur over communication mediums that allow the social engineer to disengage without ever being identified by the target.

Before exploring the source of this anxiety, the connection to excitement and thrill should be elucidated in this experience. The link between these emotions is not particular to social engineering experiences, as psychologists have noted that these two emotions share the attributes of being states of physiological arousal in contexts appraised as uncertain (Lee & Andrade, 2014). Individuals can shift between these emotions by reinterpretation of the emotion, such as through contextual cues (Lee & Andrade, 2014; Smith & Ellsworth, 1985). This connection between trepidation and excitement indicates that the factors that appear as meaningful in social engineering experiences of excitement may also reveal the source of anxiety within the social engineering experience. The morphing between the two felt experiences also points to a potential transformation of meaning that occurs within the interaction itself.

Similar to the descriptions of anxiety, social engineers identify a number of facets of social engineering interactions that are experienced as thrilling. In contrast to anxiety, this thrill is often framed by social engineers as a motivating factor that acts as an incitement to engage in social engineering. The ability to gain access to systems, to explore off limit areas, and to satisfy curiosity, appear in the narratives of the social engineers as aspects related to thrill in social engineering. The enjoyment of satisfying inquisitiveness and the thrill of finding ways of scrutinizing what was meant to be hidden parallels the hacker mentality (Steinmetz, 2015), and occurs in Zeke's narrative as an explicit comparison to the experience of hacking into technical systems.

The excitement associated with social engineering is considered intrinsically appealing and fun for many of the social engineers, beyond the appeal of simply achieving a particular goal through the use of social engineering. Just as individuals may be motivated to engage in criminal actions because of the emotional experience in the act (Katz, 1988), social engineers appear to likewise be motivated by the emotional experience of engaging in social engineering. Additionally, for some social engineers, the unpredictability and variety of experiences of social engineering mitigate against boredom and routine, and those social engineers who did experience boredom expressed that this was because the social engineering experience itself had become routine. An appeal of social engineering may therefore be the same as the theorized motivation of criminal activities, as these may act as experiences that disrupt the routine of everyday life (Ferrell, 2004).

While not all social engineering is illegal, and, in fact, many of the participants in this study describe legally authorized social engineering experiences, there is an innately transgressive quality to social engineering.[4] Just as crime may have the meaning of a transgressive rejection and resistance of societal rules (Young, 2003), social engineering can be experienced in the same way. Even in the case of social engineers who have received dispensation to engage in their actions, the licit may be experienced as illicit, as the act of social engineering often entails literally transgressing barriers to spaces and information and breaching social norms. In fact, legal social engineering experiences appear to be a means for some social engineers to have their transgressive cake and eat it too, as Victor specifically compares the interest and excitement of his legal social engineering to robbing a bank—an action he rejects because of its illegality.

In addition to the excitement that emerges from exploratory intentions, there exists another provenance from which the thrill and rush social engineering emanates. This source of excitement lies in the meaning given to the heart of a social engineering interaction: the endeavor of persuading the target of social engineering that an intentionally constructed fiction is true. The emotional intensity of this interaction is fortified by the perceptions of social engineering as challenging and unpredictable. At its core, however, the thrill of this interaction is constituted in the process of putting forward a false presentation of self or reality that the target accepts as true.

This interactional process also represents the aspect of social engineering that may be experienced with intense anxiety, absent any overt threat of conflict to the social engineer. Yet, the social engineer clearly feels that there is something of significance at stake in this interaction and is invested in the success of the interaction to the point that the meaning of potential failure can be experienced as acute anxiety and the meaning of success is felt as exhilaration. This felt experience of the social engineering interaction reveals the maintenance of face and social identity in has been imbued with great import by these social engineers (Goffman, 1956). The time investment into the creation and management of pretexts to mitigate anxiety points to this weight given to maintaining the false identity, as described by Patrick's statement that this allows him to comfortably be “that persona on the phone.” This concern with identity is additionally implicitly disclosed by several of the narratives of emotion given by the participants, while Walter explicitly makes this connection between anxiety, excitement, and the risk of exposure of a false identity.

Drawing from a symbolic interactionism perspective, this investment in a face, in a valued social identity, is conceived of as a concern with the continued existence of a self, as self-image and understandings of self are substantially constructed through interactions with others (Goffman, 1967). Experiences of social anxiety have been similarly theorized to be predicated on a concern with presentation of self in social contexts (Schlenker & Leary, 1982). The process of losing face occurs in the shattering of a social interaction, as one person is seen by the other as not actually being as they have presented themselves (Goffman, 1956;1967). If the target of social engineering detects the substantial misrepresentation of self that the social engineer has presented, either verbally or through social symbols, the social interaction disintegrates, as does the mutually construction of self that was built between the social engineer and target within the encounter. Herein lies the anxiety-producing risk that the social engineer takes when entering into a social engineering engagement.

The potential for the adrenaline rush and resulting thrill of the experience of social engineering specifically regarding the interactional dimension of social engineering takes on the trappings of symbolic edgework. While edgework was originally theorized as occurring through voluntarily engaging in activities that posed grave bodily risks, and edgework fundamentally occurs in embodied action (Lyng, 1990), further work has expanded the concept to thrilling risk-taking activities that entail contending with the risk of emotional or social harm (Landry, 2013; Worthen & Baker, 2016). Here, the social engineer skillfully dances at the edge of an interaction, maintaining control of a process that could end in the chaotic disillusion and dissolution of interaction and the sacrifice of a self-image. For social engineers who perceive their targets as opponents, successfully navigating the flow of spoken interaction, in which individuals take turns communicating with each other and parry the other's definition of reality with their own, has an additional component as not merely a triumph of self, but a victory over the other. The descriptions by some participants of targets not as adversaries on a battlefield, but as skilled competitors in a strategic game, transforms the meaning of the rhythm of social interaction into the rhythm of play—exchanging turns in a match against an opponent with whom the social engineer sees skillful strategy as the key means of winning (McDonald, 2014).

The concept of skill is a crucial aspect of both edgework and face-to-face social interaction that structures the experience of social engineering. In edgework, skill is what allows gives individuals a sense of self-control and confidence to play as close to the edge of danger as possible (Lyng, 1990). Face-to-face social interaction similarly requires the participants to use skill to maintain the flow of interchange without causing dissonance, most often by employing expressive control to prevent the exchange from being disrupted by unintended interjections of emotional expression or gestures (Goffman, 1956).

For the social engineers, the emotional experience of social engineering was felt to be contingent on both skill in emotion management strategies as well as conversational ability. Engaging in self-interaction (Blumer, 1998), social engineers would recognize their own emotional expressions, experiencing anxiety if they interpreted themselves as lacking the skill to manage the expression of those emotions, and taking action to increase their abilities. Self-assurance for the social engineers relates to self-evaluations of being able to effectively engage in social interactions, both in terms of being able to maintain the flow of conversation, as well as being able to mask expressions of emotion that cut against the reality the social engineer wants to project.

Conclusion

This analysis of the felt experience of engaging in social engineering points to several implications. First, multiple motivations are revealed to be possible enticements for the social engineers to engage in social engineering, in contrast to the motivations for material gain typically assumed in the literature. While monetary gain may be a component of the motivation to enter into social engineering, the experience itself often provides an emotional reward to the social engineers. It is not simply that these additional motivations should be recognized in examinations of social engineering, but that these motivations appear to be differentially distributed across mediums of communication that allow for more or less social distance from the target of social engineering.

Social engineers who are attracted to the experience of thrill and adrenaline rush in social engineering should theoretically be drawn to more personal, direct forms of communication, such as face-to-face or through phone calls. In contrast, social engineers who experience social engineering as a mechanism to achieve a goal beyond that of the experience itself would theoretically be more inclined to use more indirect mediums of communication to avoid to the challenge and potential anxiety generated within more personal interactive contexts. Future research delineating social engineering motivations across communication methods may be valuable for organizational policy.

Chapter 5 - Analysis: Maintaining Deceptions

While the previous chapter examined the emotional experience and motivations of social engineers as they engage in social engineering, this chapter will analyze how social engineers and security auditors work to maintain deceptions throughout their social engineering attempts. This analysis lends insight into the ways in which social engineers exploit interactions and social systems, which, when successful, allows for the creation of near perfect fabrications. There were two main themes within the analysis. The first theme delineated two categories of deceptions which required distinct forms of maintenance by social engineers. The first of these deceptions is active deception, designated here as *bluffing*, and covert deception or *stealth.* Participants described how social engineers could employ either, or both, of these forms of deception across the course of a social engineering attempt. This results section will first elaborate on the maintenance and implementation of both these forms of deception by social engineers. The results will then turn to the second theme of *social technology for the maintenance of deceptions,* which examines the advantages and challenges posed to deceptions in social engineering attempts through the use of technological forms of communication as well as the role played by organizational and societal structures.

Bluffing versus stealth

The results reveal two overarching genres of deceptions employed by social engineers, which required distinct forms of maintenance to keep from collapsing. The first category of deception is bluffing, in which overt falsehoods are presented as reality in interactions with targeted systems or individuals. In this form of deception, the fabrication presented by the social engineer tends to be embedded in the communication itself. By bluffing, the social engineer actively engages in a charade by verbally, or in writing, presenting a lie as the truth. This legerdemain is fundamentally interactive, as the social engineer presents a deceptive narrative in the hopes that another person will accept the narrative; failing to detect anomalies that could cause fabrication collapse. According to participants, maintaining bluffs could be as straight-forward as flashing a fake badge at a security guard while walking through the doors of a secure facility. However, maintaining bluffs also occurred in elaborate, dynamic series of interactions, in which the social engineer attempts to deftly evade detection by accounting for potential anomalies that could lead to the collapse of the fabrication.

The second of these two categories is stealth, in which a social engineer attempts to avoid interactions and queries that could lead to detection by evading the notice of the targeted individual, system, or organization. This form of covert deception closely resembles deceptions by omission (Leal, Vrij, Deeb, Hudson, Capuozzo, & Fisher, 2020), in which crucial information is withheld to cause someone to believe something untrue. In the case of stealth, the social engineer attempts to withhold and suppresses potential indications that subterfuge is underway. In these clandestine deceptions, there may be no interaction, as the social engineer may slip into a protected space, physically or technologically, without directly communicating with another person. In contrast to the explicit chicanery that required a proffered narrative to be accepted for the deception to continue, covert deceptions rely on avoiding producing anomalies that could bring attention to the social engineer. Forrest highlighted the difference between these forms of deception by saying:

> I'll make an analogy in the insect world, the animal world, you can either be an insect that tries to blend into his or her surroundings and not become prey, or you want to be so ostentatious in your adornment and coloration that you catch the eye of a bunch of other living creatures… And I think those are the two classifications of technique that will

> apply in social engineering. You either want to blend into the landscape or you want to go big and be, be noticed in a way that spins people's head and throws them off their regular cognitive process.

The former deception characterized by active chicanery is explicit, as the deception is presented to an individual for evaluation for anomalies. The latter is implicit, as the deception is an attempt at covertly achieving some goal without being confronted.

Bluff

In the active form of deception in which the social engineer puts forwards a false narrative as true, anomalies that could result in the failure to maintain the fabrication tend to be embedded in the context of the narrative or message itself. Victor describes the process by which he thinks through deceptions to avoid producing anomalies. He says:

> So like in the terms of getting credentials, you know, you can use a phishing email or you can use a, you know, where you call them directly and, you know, the popular one is you're posing as IT. And it's like, "Okay. Would IT really call you and just ask for your password?" …And the person's password that I'm getting, are they somebody who would have access to the kinds of information I want? ...So depending on what I'm trying to access, whether physical, digital, whatever, and then figuring out who would normally have access to that stuff, and then manipulating them to also allowing me access.

Crafting a deception, within this context, involves evaluating whether the communication will be seen as plausible to the target or whether there are potential anomalies that might need to be mitigated against or resolved. In his description, Victor expresses concern that there could be anomalies detected in the identity that he plans on purporting to have, in this case an IT professional, as well as the narrative that solicits information from the target. Although not explicitly stated, Victor's approach of "figuring out who would normally have access" to the information he seeks relies on assumptions about general organizational policies and the trust that individuals place expert systems (Giddens, 1990) that exist across modern society. For the bluff to be maintained, Victor must present himself and his requests as within the norms of what his targets would expect from a professional, such as an IT professional.

One of the more basic forms of bluff described by participants were phishing emails, which tended not to involve extensive maintenance, but were overtly false narratives presented to targets as truthful. Jerry emphasized the effectiveness of a sending simply worded emails, saying: "'Hey, your bank password has expired after 90 days. Please change. Click on this link to do so.' More effective than anything else." However, more dynamic forms of bluff relied on the social engineers being able to maintain the deception across the course of an interaction. Arlo elaborated on a specific incident in which a fabrication collapsed during this manner of deception. He described a situation in which his wife was speaking to scammers who called and claimed to be from the IRS:

> And they started yellin' at her and gettin' her upset and she's going along and all of a sudden they start asking for credit card information and she's like, "Whoa-whoa-whoa. I don't give out credit card information over the phone to people who call me." And then all of a sudden they yelled and screamed at her, said, "We're filing an arrest warrant now," and hung up on her. So she calls me in tears and stuff and I was like, "Hold on. Let me check it out." So I call it up and right away I knew what was going on. Like just by the cadence and the accent and you could tell that they weren't American. It was very obvious that they didn't work with the IRS.

There are two points in Arlo's account of this deception in which anomalies were detected that led to the scammers failing to maintain their deceptions. The first occurred when they requested a credit card payment from Arlo's wife, who appears to have been unsure as to the legitimacy of the callers, but who asserts that she will not give out credit card information over the phone. In this case, the request and stated identities in the deception could not justify the anomaly of a credit card payment across this technological communication medium. The second anomaly that resulted in the total collapse of the fabrication was that the narrative being presented by the scammers did not match Arlo's conception of how an agent from the IRS would act and speak in a phone call, after which point the deception could not be maintained.

Stealth

Covert deception, in contrast to overt bluffing, generally involved the social engineers attempting to maintain deceptions by avoiding creating anomalies that would lead the collapse of their fabrications in the revelation of their illegitimacy in the spaces that they were trying to gain access to. Ida expressed this concern by stating: "You have to adopt this kind of like, 'Don't pay attention to me,' gray woman or gray man type of persona, and that definitely helps when I am, when I am on an engagement. I am able to blend in with the rest of the crowd entering a building." She further elaborated on how she thinks about being detected in social engineering engagements where she's attempting to be covert, by saying:

> Most people, you pass them in the hallway, they'll smile and walk by, or they'll briefly make eye contact with you and then turn back to what they were doing. If somebody makes eye contact with me for longer than that brief glance, that brief momentary glance, it probably means that they recognize I, that I'm, I'm new, that they've noticed me, and that is always a little bit concerning. That means that I need to get, polish up my pretext (laughter) 'cause I'm probably gonna be doing some talking.

By analyzing the body language of those around her, Ida attempts to evaluate whether her presence is being seen by others as anomalous, or whether she is successfully blending into the crowd. In particular, Ida's focus on the meaning of eye contact is reminiscent of Elijah Anderson's (2011, p. 113) concept of 'eye work,' in which strangers in public urban settings adhere to an unwritten codex of norms surrounding appropriate ways of looking at strangers that indicate civility, in contrast to forms of eye contact (i.e. prolonged stares, glares) violate civility and signal potential threat. Despite the fact that Ida is not engaging in overt bluffing in her example, her description of maintaining deception by stealth is fundamentally interactive. Not only does she attempt to parse the intentions behind the eye work and body language she sees in others as she passes strangers in the hallways, but she also attempts to 'blend into the crowd,' by not drawing attention to herself in her own body language and demeanor.

The importance of body language during some furtive attempts at deception was also emphasized by Tara who said:

> I usually watch the eyes of the people around me. You can tell when they're getting suspicious, they kind of start shifting, like their eyes get really shifty, and if one, I guess the branch manager or whoever's in charge kind of sneaks off to their office then I just think they're about to call the police.

Social engineers also described maintaining a false presentation-of-self as both a form of overt bluff and covert deception across different interactions within a social engineering attempt. Lucy described an example of such an engagement, in which she presented herself as a supervisor in a landscaping company. She described how she thought of this deception: "…as I did my recon, I thought, "…who's invisible at a place?" … while I was doing recon, actually, the landscaping crew came to do the maintenance so I got to see who they worked for, what they wore…" After dressing to appear as though she worked for these landscapers, she entered the building elevator and almost immediately must engage in overt bluffing to maintain her deception when an employee began speaking to her:

> When he, you know, talked me, I said, 'Oh, you know, I'm just here to check on how the landscaping has held up.'…And, so he actually escorted me to the area so I could go look at the plants. He'd asked if I wanted to see the, talk to the facilities manager and I said, 'Nope,' I just needed to get out to the terrace and that was it.

Once Lucy had access to the level of the building that she needed to compromise, she continues her deception covertly, as she had initially planned. She describes this covert stage of the engagement:

> I stood there making notes on my clipboard about what I'd, you know, what I'd seen in the plants and so people ignored me. They saw me but they ignored me… Because of the general invisibility of people like landscaping staff.

When covert deception is no longer a viable option to maintain the fabrication, it may be followed by active bluffing. In fact, several participants described planning social engineering attempts in which they had planned initial stealth deceptions, but had also prepared 'backup bluffs.' These backup bluffs allowed them to rapidly dispense with attempts at stealth, rather than attempting to maintain this form of deception if its authenticity appeared to have become overly tenuous to the target. A security auditor, Zeb, described a specific social engineering experience in which he attempted to covertly gain access to an office in a physical penetration test. To avoid the collapse of the deception should he be confronted by someone in the office, he crafted a pretext around being an Energy Star Compliance contractor and researched what this role would entail. He described both the attempt at surreptitiously entering the office, as well as deploying his pretext when confronted. Zeb stated:

> I went into the building around noon when I knew that the secretary was not gonna be there, just so I could wander around their open space and kind of check things, and then if someone approached me I was going to tell them why I was there, and what I was doing, and why I was supposed to be there. Which is what I did. And someone told me that they, that I needed to talk to their facilities manager so they brought their facilities manager down, and then I just laid everything on her as hard as I could, giving her random stuff about energy star compliance and different kinds of ways to save energy, and anything and everything I could think of that would be in that realm just to really sell it hard that I was with Energy Star.

Here, the attempt at covert deception is transformed into a deceptive narrative about an identity that reasonably accounts for his presence in the office, allowing Zeb to maintain his deception without causing his fabrication to collapse.

Regardless of the form of deception undertaken by the social engineer, the ability to maintain these deceptions relies, in part on external organizational and social context that the social engineer operates within. This context can be used to the social engineer's advantage and allow them to effectively maintain their deceptions, or it may pose challenges that allow anomalies to be more easily discerned by those targeted by these deceptions. The results will now examine aspects of this external context that were highlighted as important by participants.

Social technologies in the maintenance of deceptions

The results indicate the significant role played by social technologies in the initial viability of social engineering deceptions, as well as in the maintenance of such deceptions. The concept of social technology is term that has been loosely applied in divergent ways in different contexts. Participants described two dimensions of social life which could be conceptualized as social technology. The first of these is invoked by Karl Popper's (1947, p. 18) concept of social technology, which describes how institutions and culture can be used as tools to sway the behavior of individuals and societies, as well as the more generic modern usage to refer to technologies used for communication (Harrysson, Schoder, & Tavakoli, 2016). These social technologies include broad cultural and social systems and occupational and organizational norms and policies that social engineers use as tools to hone their deceptions. In addition, social technologies refer specifically to forms of communication mediated through technology. Both of these social technologies provide a route that could either bolster fabrications and allow them to be maintained, or could cause the collapse of the falsehood. Participants described two circumstances in which fabrication failure could occur: during active subterfuge, or during attempts at stealth in social engineering.

Technological forms of communication

When social engineers failed to maintain deceptions, participants described the crux of this failure as often lying within in anomalies within the pretext created by the social engineer. Social engineers utilize varying means of technology to craft and convey deceptions, and within each communication medium there are specific types of information available for evaluation across the interactions, depending on the form of communication. In social engineering deceptions occurring within email, for example, participants described relying on information about the email sender's identity and the written content of the email to evaluate the potential for deception. Ann elaborated on detecting deceptive emails, saying, "They're, maybe they're, the format of their email looks weird, or their grammar and syntax is poor, or they're coming from an email address that that organization doesn't usually communicate with you on, or coming from a phone number that they, that organization doesn't usually call you from." Here, the potential to for the deception to fail to be maintained occurs in the examination of the substance of the message and any notable characteristics of the source of the message. Cecelia also discussed determining whether emails contained deceptions within her organization:

> So the business email compromise one, attempts that we have is, you know, like they want someone to pay for an invoice, and there's people who are very familiar with the process, and it's not coming, if it's not coming from, you know, someone in upper management, they say that they look at the email and they're goin', "That's not even one of our emails," and, you know, forward it over to us…

The ability to for the deception to be maintained is dependent on the content of the messages containing anomalies that can be detected. In this form of communication, the message is scrutinized for anomalies, as the social engineer can shroud their identity by using a communication medium that conveys limited information about the sender.

In contrast, social engineering attempts via email were described as evading detection and being maintained when the message contained no anomalies that could be detected. Such an email is described by Gerald, who said:

> …I found what an internal email looked like on the client's webserver, the server. And, so I took a copy of that and handed it to, you know, our guy that's way more into design, you know, he's way better at that and, you know, we were able to put together an email that looked exactly like theirs.

In this context, fabrication failure is unlikely to occur, as the email has been crafted to eliminate potential anomalies that could be used to detect the deception.

When social engineering occurred across phone calls, deception detection could occur in a similar manner as in emails, but there is also additional information, such as tone of voice and speech patterns, that social engineers convey. In communication mediated by email, vocal information would not be available for evaluation, though the written content of the email could be stylistically different from the sender's standard communication style. Zeke, a security auditor, provided an example of failing to maintain a deception that occurred in this communication medium during a social engineering campaign he was conducting. He said:

> …We called the data center folks and said, 'cause we had a company directory right in front of us, and we're like, "Hey, you know, just so you know, this is so-and-so, I'm in charge of security, you know, we have a few folks coming down there for PCI, the payment card industry standard, you know, to do an assessment, can you walk them through, you know, the data center?" He's like, "Who did you say this is?" I'm like, "Oh, you know, Bob, you know, whatever, Smith. Bob Smith." "You know, hey, I'm good friends with Bob and you're not Bob." You know, like, "Ah, shit," you know, and you hit the button real quick, you know, you hang up and you run, you know?

The fabrication created by Zeke failed as the individual on the other end of the call became aware of an anomaly that made it clear that the interaction was deceptive. Because this communication occurred over the phone, Zeke's impersonation attempt failed as the person with whom he was speaking recognized that that he did not sound like the person who he was claiming to be.

In in-person social engineering, fabrication collapse tended to center around anomalies in the social engineer's behavior in a space, or failure to justify their presence in a restricted area. Zeb describes such a fabrication failure during a physical penetration test he was conducting as part of a security audit in a building which required badge access. He recounted:

> But on the third floor, they had badge access to get out of the staircase. As I approached the door to go through it, there was another gentleman coming out so I kind of hid off to the side real quick, played around on my phone, he came out, I grabbed the door and went in. He came back in and approached me and was like, "Hey. Who are you? And where are you supposed to be? And why are you here?" And at that time like the, just the timing of all of it, I had no good response for him so I just revealed myself to him and said, "Alright. You caught me. I'm, here's my get out of jail free card."

Because Zeb needed to wait until the door was opened by an employee in order to gain access, he engaged in an anomalous behavior that was interpreted by an employee as indicative of deception. Once this anomaly was detected, he was unable to provide an explanation that was sufficient to account for the anomaly and maintain the deception by assuaging the suspicion of the employee.

In contrast to Zeb's failure to be able to justify his presence, which resulted in the failure of his fabrication, when potential anomalies can be accounted for by the social engineer, then fabrication failure can be prevented. Malcolm provided an account of such a circumstance that occurred during a social engineering engagement in which he was performing a physical penetration test. He said:

> …Somebody had approached me at one point during the thing and questioned me on what I was doing there and so I, just thinking on my feet, I just explained to them that I was working with so-and-so, that I just picked a name out of a hat that was one of the people that was working there… enough people [were] working at the branch and they were in a different department, I figured, you know, probably wouldn't actually know that…and said I was workin' with them to get a new account set up and I was just entering some information. They're like, "Oh, okay." And then they, they just left me alone. And, so then I just finished entering, finished doing what I needed to do on the computer and got out of there. And that was, that was that.

In this case, an employee thought that some aspect of Malcom's activity during the social engineering engagement was anomalous enough to approach him and question him about what he was doing. As the social engineering was able to provide an adequate account of his presence within the organization, he was therefore able to avoid the collapse of the deception and to continue with the social engineering engagement undetected.

The medium of communication used by social engineers shapes the ways in which they attempt to maintain deceptions during social engineering, as well as impacts the potential points of failure within the deception, as certain types of anomalies may occur more easily or become more difficult to justify to a target. In addition to the form of communication used to convey a deception, participants identified broader social factors, including institutional and cultural norms, governmental regulation, and organizational culture and policies that also shaped how deceptions were maintained.

Social factors impacting deception maintenance

Social structures and cultural norms and values were described by participants as factors that, depending on their specific qualities, could either facilitate or challenge the maintenance of deceptions in social engineering. For example, legislation could be in place that created substantial barriers to particular types of deception, or such legislation could be absent, creating a situation that facilitated the ease with which a social engineer could maintain deceptions. Participants emphasized two ways in which these social factors could impact the maintenance of deceptions—some social factors had an impact on particular domains of information and posed an equal challenge to all social engineers, while other social factors were related to characteristics of individual social engineers. The first form of social factor will be examined, prior to elucidating the factors that were contingent on personal characteristics of the social engineer.

Participants described social factors, such as legislation and organizational cultural standards, that made targets of social engineering either more or less susceptible to social engineer deceptions as a whole. Governmental regulations and policies represented a social factor that influenced social engineering deceptions as a whole, regardless of the specific characteristics of the social engineer. Regulatory policies were implicated in structuring how social engineers maintained deceptions by both participants who engaged in social engineering, as well as IT professionals tasked with ensuring regulatory compliance. Lucy, a social engineer, described the impact of regulations regarding medical and educational information as follows:

> Like if I'm trying to get information that is sensitive from a HIPAA perspective or a FERPA perspective, that tends to be a lot harder because the people who deal with that usually because that's, maybe like funding issue, either from I get to keep my funding like with FERPA or HIPAA, I wish to avoid fines - there tends to me more training around that particular type of sensitive information and so that tends to be a lot harder to get at because there's a lot of focus on it.

The above quote attributes the difficulty in deceiving targets who use this type of information as due to the focus that the regulations put on protecting information in these areas. Lucy also points out that organizations are financially incentivized to protect this information because of the penalties associated with failing to do so. Ernest, an IT professional, pointed out that regulations did not simply change the awareness and incentivization of potential targets, but also had implications for the technical data infrastructure that would make create a greater challenge for unauthorized access to occur: He said:

> We create sandboxes, so to speak, within the network, around the different levels of data. So when you're dealing with anything that is HIPAA related, we keep a sandbox of security around that…so each one of these we do keep in separate distinct areas that the permissions are managed at the user level and the data level. So we try to hit that and then a tremendous amount of training and reinforcing of those….of individuals using the systems so that they are constantly aware.

Although Ernest does not explicitly state the consequences of these data governance policies for social engineering deceptions, the implication, suggested by Lucy, is that these types of regulations inhibit the ability of social engineers to present deceptions that would be possible maintain to access information in these domains. While regulations may protect HIPPA data within a network by limiting the number of users who have permissions to access the data, thus limiting the pool of potential targets and deceptions that a social engineer could use, such information is not made inviolable by these regulations. Bernard, a social engineer, specifically identified hospitals as often deficit with regards to physical security procedures, stating:

> In a hospital, hospitals in particular are so chaotic that when you walk in, you almost, you have to be willing to just improvise and take what you see because you'll be walkin' up a hallway and there's a, what they call WOW's, or work station on wheels just sittin' there unlocked, wide open, with patient information on it. You're not gonna walk by that.

HIPPA information being exposed via workstations within a hospital provides a route for social engineers to construct and attempt to maintain a deception in a physical setting, even is such a data system that was compliant with federal regulations and might be difficult to access externally. The regulations may therefore structure the process by which social engineers maintain deceptions by shaping the circumstances in which it is plausible for a deception to be maintainable.

Organizational culture and policies were also highlighted by participants as a social factor that broadly structured how social engineering deceptions could be maintained. For some participants, organizational norms could be generalized across an entire industry. According to David:

> There's certain organizations that have absolutely no security awareness. I mean, that's, and that's pretty obvious just in, say manufacturing. Manufacturing plants have no security awareness…Those would be, honestly, you'd be able to walk in and walk out with whatever you want.

Although David uses the term 'security awareness' without specifying the particular organizational polices or practices that would result in security awareness, it is clear that he understands the manufacturing industry to be susceptible to social engineering deceptions and that maintaining such deceptions would not be challenging. The identification of industries with policies and norms that impact the ability of social engineers to maintain social engineering deceptions was also expressed by Clarence's statement that, "So, you know, government type targets are a little more difficult to get into."

The culture, policies, and practices of individual organizations could also shape social engineer's maintenance of deceptions. Bernard gave an example of such a company, saying:

> I was an internal auditor for a construction company, and they were an old company… I put on a shirt and tie and went down there…and walked into the first office I saw, walked up to the little security, or not security, like the admin assistant who was sittin' there and said, "Hey, I'm from IT and I'm here to pick up," and I read the name off the office behind hers, "computer." And she said, "Alright. Go ahead." And I went and grabbed the laptop, walked out the door… I didn't even do any pretext or anything. I just went down after lunch with a tie on, 'cause I knew they all wore ties down there.

While the industry of the company is noted, what is described is the lack of policies in practices within this particular organization that allowed the social engineer to easily pose a deception that was accepted without being seen as anomalous to the administrative assistant encountered during the social engineering engagement. Notably, while Bernard states that he did not use a pretext during this deception, he in fact, did use the pretext of being from the IT department, which validated both his presence and apparent legitimate access to the laptop. The success of such a rudimentary pretext that the social engineer is disinclined to acknowledge it as such, points to the ease with which he was able to maintain the deception within the organization.

Social engineers also discussed social factors that could be assets or liabilities to their own, personal ability to maintain a particular deception while engaging in social engineering. An aspect of Bernard's description of illicitly acquiring the laptop during his social engineering attempt additionally illustrates a way in which social technologies can impact the ability of an individual social engineer to maintain a deception without appearing anomalous to the target. As part of his pretext to appear from the IT department of the company, he puts on a tie, which he intends to mark him as a member of the organization, who also wear ties, and which more broadly serves to indicate that he is part of the white-collar workforce, which may grant him some degree of social trust as part of an expert system within society (Giddens, 1990).

The tie, however, cannot be assumed to act as a talisman that a social engineer could employ to maintain deceptions in all in-person settings, but rather belongs to a broader category of props that social engineers may employ to maintain deceptions within certain contexts. Zeb describes the similar use of attire as props to signal membership in blue-collar labor in an social engineering deception in which he gained access to a power plant. He said, “That guy came down to the guard station, kind of checked me out real quick. I was dressed like them, you know, a polo maybe or a button-up and jean and work boots, and I had a hardhat that had their logo on it.”

The use of props, such as hard hats and ties, in the maintenance of social engineering deceptions echoes Goffman’s (1959, p 24-26) description of how props are employed to maintain social fronts, which are the cultural expectations surrounding how individuals in established social roles should appear and act. As Goffman (1959, p. 27) states, “It is to be noted that a given social front tends to be institutionalized in terms of the abstract stereotyped expectations to which it gives rise.” This statement implies that when social engineers attempt to maintain a deception that they have membership in an expert system through the use of props or modifications of appearance, they are attempting to portray themselves in alignment with a stereotypical set of expectations that their targets may have about that role. In this case, aspects of the social engineer’s individual identity may impact the extent to which they are able to maintain particular deceptions. Gerald illustrated this phenomenon in his discussion of a female social engineer’s strategies in choosing pretexts: “If she says she’s in IT that’s gonna throw up a lot of red flags with people. But that’s the stereotype. But if she says she’s a receptionist, you know, well absolutely, of course you are.”

In addition to societal expectations that structure the social roles individual social engineers may attempt to fabricate membership within, social technologies within cultures, particularly language, could pose barriers to the maintenance of deceptions by individual social engineers. Brian gave an example of the significance of language in maintaining deceptions, in saying:

> Like I've tried to infiltrate Russian websites that talk about malicious stuff and they've caught me using Google translator. You know, 'cause I don't understand the slang. So I Google translate and I'm not speaking slang, I'm speaking straight up Russian and translate the probably wrong wording of things, and they've called me out and blacklisted me.

This example illustrates a profound deficit in language ability that prevented Brian from being able to maintain his deception because he was unable to convince his targets that he shared their cultural background.

Discussion

Social factors, such as cultural expectations, and social institutions shape the extent to which social engineers can maintain deceptions with ease. Participants expressed that these social factors, in addition to communication technologies, structured the circumstances in which social engineers could interact with their targets and thereby also their options for maintenance of the social engineering deceptions. Within these contexts, social engineers attempted to maintain either covert or overt deceptions. Covert deceptions, or stealth, consisted of social engineers who sought to maintain the deception of legitimacy through evading notice. Overt deceptions, or bluffing, consisted of direct communications in which social engineers falsely assert a legitimate claim to access protected information or domains, often by falsely representing their identity.

Theoretical implications

The theme of covert, stealthy deceptions is of theoretical interest from an interactionist stance. The maintenance of a deception necessitates the continuation of a targeted entity or individual being deceived, yet the social engineers seek to avoid and minimize potential interactions within this form of deception, rather than seek to convince targets through communication. This form of covert deception elicits theoretical similarities to Goffman's (1969, p. 12) discussion of control moves, which he defines as "the intentional effort of an informant to produce expressions that he thinks will improve his situation if they are gleaned by the observer." A specific variety of control move within Goffman's framework is a 'covering move', which includes a range of behavioral strategies to keep information secret. These stealthy deceptions appear to fit within the category of 'covert concealments,' also referred to as 'camouflage,' in which the deceiver attempts to keep hidden the knowledge that there is information that is being withheld (Goffman, 1967, p. 14).

The results point to social engineers exploiting normative organizational and social structures to avoid drawing attention to themselves as they attempt to blend into background social processes. At an organizational level, these attempts at camouflaging deceptions might be characterized as exploitations of situational normality and structural assurances (McKnight, Cummings, & Chervany, 1998). Situational normality fosters trust within an organization when the interactions that individuals have within these settings appear typical of what those individuals would expect, based on organizational norms, policies, and past experiences. Structural assurances include knowledge of organizational regulations that ought to structure the behavior of individuals within these organizations (Mcknight, Cummings, & Chervany, 1998).

For both stealth and bluffing, which fits into the covering move Goffman (1967, p. 14) refers to as ‘misrepresentation,’ the participants appeared to utilize expert systems to either evade attention or to bolster their bluffs. Giddens (1990), drawing from Goffman, describes faceless commitments, which are characterized by trust of abstract systems in which social relations have become disembedded from time and space, and experts must often be trusted as having effective technical knowledge based on the system that trained them, rather than by an awareness of their quality through personal interactions. This form of faceless commitment is illustrated by Zeb’s description of a social engineering engagement in which he pretended to be an Energy Star Compliance contractor. Through his supposed affiliation with the Energy Star program, Zeb relies on his targets’ trust in expert systems that he exploits to pose as though he has a legitimate need to enter the building to promote energy efficiency.

Giddens (1990) highlights that trust may be bolstered or compromised at access points where individuals engage in facework as representatives of faceless expert systems (Giddens, 1990). Thus, the way in which social engineers present themselves, as well as their appearance can impact their ability to maintain deceptions. Bernard, for example, describes wearing a tie and intentionally presenting himself in a manner that was reminiscent of the workers within the organization that he was targeting to maintain trust. Both trusting and having been entrusted signify particular relational meanings and emotions, with interpersonal trust relations having the most emotional significance for individuals (Jones, 1996; Lewis & Weigert, 1985).

The context in which maintaining deception social engineering interactions occurs can therefore be understood as intertwined within the conditions of modernity, as individuals evaluate whether they can trust the communications of individuals, who are often unknown to them, but who represent themselves as part of the expert systems by which society is structured

(Giddens, 1990). Both covert and overt deceptions by social engineers may rely on representing communications or selves as components of expert systems; where a covert deception may be created for the purpose of blending into an expert system, while an overt deception might explicitly claim membership in the expert system.

Information security awareness implications

Social engineers who deploy deceptions under favorable external conditions and who effectively utilize social technologies, including expert systems, may create near-perfect facsimiles of authentic communications, which provide no anomalies to detect, regardless of the incredulity of the target or the level of knowledge that the target could draw upon. A similar characterization of these deceptions framed them, not as indistinguishable from genuine messages, but as appearing sufficiently authentic to fail to evoke suspicion from a standard level of scrutiny from a trained, relatively knowledgeable individual.

The process of maintaining active bluffing deceptions is characterized by what Goffman (1974) calls moves and countermoves. When the social engineer presents information that is not congruent with the target's understanding, the targeted individual, sensing an anomaly and becoming doubtful about the veracity of a situation, seeks authentication (countermove). The fraudster then may attempt to provide some kind of authentication or excuse (a counter-countermove). This attempt may fail, causing the deception to be immediately discredited. The authentication can also succeed, which may engender trust and the continuation of the deception. Even after authentication, however, an individual might remain suspicious of the situation. To counter being taken in by false authentications made by social engineers, the results highlight that individuals can draw on knowledge about how social engineers operate and how they structure deceptions. Joan suggests this when she says, “don’t ever allow anyone to authenticate with you on something that is publicly available.”

Even while there is potential for deception detection to occur through the deft use of knowledge within these iterative interactional exchanges, both the participants in the current analysis, as well as the deception detection literature indicate that while knowledge regarding a situation can improve accurate deception detection, a substantial error rate remains (Blair, Levine, & Shaw, 2010). ‘Near perfect’ fabrications presented by social engineers in this context may be close to indistinguishable from authentic communications, leading to a situation in which deception detection is contingent on the quality of the deception, rather than the evaluating abilities of an individual.

These findings are reinforced by the literature, which has found that susceptibility and resistance to security threats may be influenced by trust within organizations. At a fundamental level, it has been argued that trust between organization members is required for organizations to effectively operate (Chan, 2003; Dirks & Ferrin, 2001; Mayer, Davis, & Schoorman, 1995). A dimension of trust between workers that has been posited as of particular influence within organizations is managerial relationships with their subordinates. Particularly hierarchical organizations may often require trust from subordinates by expecting authority figures within the organization to be deferred to and obeyed without explanation (Kramer, 1999). On one hand, this may be beneficial for social engineering resistance by restricting the spread of information within an organization that could be exploited by social engineers. On the other hand, however, social engineers could exploit this trust in organizational authorities through impersonation of such an authority. Mansfield-Devine (2016) provide an example of this type of trust exploitation can be seen in

CEO frauds, in which a social engineer sends emails to accounting employees masquerading as an executive and requests money to be transferred.

Chapter 6 - Analysis: Deception Detection

While the previous two chapters focused on the experiences of social engineers in engaging in social engineering and maintaining deceptions, this chapter turns to examine how the targets of social engineering can detect such deceptions. The results of this analysis are based on the full sample of interviews (non-professional social engineers, security auditors, and IT professionals; n = 54). While the entirety of each interview was analyzed for content related to deception detection in social engineering interactions, there were several questions within the interviews that evoked most of the participant discussion of situations and experiences related to detecting deceptions that occurred during social engineering such as, for example:

- "If you were to give advice to someone about how to avoid being socially engineered, what would you say?" (all participants)
- "Have employees in your organization ever been subject to social engineering scams targeted toward getting access to your IT systems?" (IT professionals only)

An additional area in the interviews that provided relevant material for this analysis were descriptions of social engineering interactions in which social engineers describe either failing or succeeding in deceiving individuals.

Two primary themes emerged in the analysis of deception detection in social engineering interactions, both of which were framed by participants as means of contending against or mitigating perceived barriers to anomaly detection in individuals. The first of these themes was that of *individualized* anomaly detection strategies, which is composed of three subthemes, each of which are characterized as strategies intended to increase the agency of individuals targeted by deceptions. These three subthemes are: perceptual strategies, cognitive strategies, and knowledge-based strategies. Each corresponds to a perceived weakness that could prevent a person from becoming aware of a deception and an associated strategy to bolster their alertness. Cognitive strategies focus on thought processes often described by participants 'critical thinking.' Perceptual strategies refer to attitudinal stances and actions individuals can engage in to contend against accepting potential deceptions as true without sufficiently interrogating the claims being made. Lastly, knowledge-based strategies were said to involve providing individuals with information useful for situating potentially deceptive requests and communications into a broader organizational or institutional context, which could point to anomalies in the deception. In short, individualized anomaly detection strategies involve improving the ability of individuals to perceive interactions as potentially deceptive, identify the markers of potential social engineering attacks, and cognitively process social interactions in a manner which reduces the likelihood of deception. The perceptions, skills, and knowledge, required by individuals can also be externalized, however, shifting the responsibility for deception detection away from potential targets themselves to experts, a strategy described here as *outsourcing*, or technological solutions, termed *automation strategies*. Both outsourcing and automation thus constitute *externalized anomaly detection strategies.*

Individualized Anomaly Detection Strategies

Individualized anomaly detection strategies were framed by participants as methods by which individuals could better hone their ability to detect deceptions while enmeshed within an interaction with a social engineer. The ability of individuals to detect deceptions in social engineering interactions was framed by some participants as contingent on the recognition of anomalies in the way in which social engineers presented themselves or in the messages sent by social engineers. Anomalies consisted of unexpected features of the social engineering interactions. Examples include unusual requests, or messages that would be atypical from the purported sender in terms of content or writing style.

Individual capability to discern anomalies was attributable to one of three individualized strategies, according to participants. The first of these are perceptual strategies used to contend against being overly trusting and willing to follow directions deceptively proffered by social engineers. The next subtheme is that of the cognitive strategy of evaluating situations for anomalies, which tended to be generically referred to as "critical thinking." This strategy was characterized as allowing individuals to actively evaluate messages and interactions with social engineers, in contrast to passively accepting a potentially deceptive narrative. Lastly, knowledge-based strategies were imputed to be a significant aspect of detection of anomalies, as individuals with knowledge of relevant domains were seen as being more able to detect anomalies in patterns. Although each of these subthemes were distinguished by participants as components that allowed for the detection of anomalies in social engineering interactions, all the subthemes are interrelated with one another and are used in conjunction in the process of deception detection.

Perceptual strategies

Perceptual strategies were framed by participants as an approach to interactions and communications in which an individual assumes that there is potential for deception to occur, in contrast to an assumption of implicit trust within the interaction. Perceptual strategies could take the form of attitudinal stances of skepticism as well as consist of actions that might be taken by default to authenticate the legitimacy of an individual or communication that could potentially be deceptive. Having an appropriate perceptual strategy was framed by participants as a prerequisite for the effective use of either cognitive or knowledge-based strategies in deception detection.

According to participants, without appropriate perceptual strategies, many individuals are left susceptible to deceptions due to having overly trusting dispositions or being overly willing to believe in the legitimacy of interactions without question. Trust dampens the perception of a target that a cognitive or knowledge-based strategy is needed to verify the accuracy of potentially deceptive communications. Therefore, participants often contrasted action on the part of the target with trust, which was associated with a lack of action to evaluate a potential deception.

The use of percentual strategies is set against willingness to trust, which participants differentially attributed to either individual disposition or to cultural norms. Some participants characterize the desire to trust as a part of human nature. For example, Herbert said:

> You know, it's human nature to want to trust people, especially, you know, people with, just with the social media… I'd say you got to keep your guards up, you know, and, yeah, you don't want to trust everyone. But, I mean, you don't want to block anyone out, you know, you don't want to have a wall up.

Cultural explanations of the propensity to trust were also given by participants. Cecilia made such as statement: "…we are a nation that we trust people at the core, you know, because we want to build that relationship, we want to build that rapport. You know, understanding different personalities that are out there, that comes into play." Although participants attributed the source of trust to differing sources, such as an innate attribute or an organizational or cultural norm, there was a consensus regarding the significance of the role of trust in failing to detect anomalous interactions.

Jeremiah discussed the importance of employing perceptual strategies to mitigate against implicit trust with regards to social engineering and said, "Trust no one…It all comes down to trust and where you want to place it. At some point, you have to have trust somewhere, and I understand in a world where you can't trust anyone, it's very scary and it's very annoying." The percentual strategy of being aware of the exploitability of trust and seeking to be less credulous does not ensure that deceptions will be detected in actuality. Rather, these stances provide individuals with a defensive perspective that allows them to take time within an interaction to evaluate it. John characterizes this quality as skepticism when he says:

> …you want to be naturally skeptical. If somebody says they're supposed to do something, your first reaction should always be no… 'Wait a minute. I don't buy anything at Target. Why did Target send me an email? I'm not clickin' that. That can't be right.' I don't care if it says if my order is ready for pick-up, you know, or I don't, it is really, for people to stop and think and ask the question, does this even remotely make sense?

The anomaly of an atypical message that supposedly originates from Target is ascertained by an individual because of their incredulity towards the message; a stance from which the person can pause to assess the incongruities within the situation.

Furthermore, the importance of utilizing perceptual strategies to maintain an assumption that an interaction could be deceptive is highlighted by the participants who engaged in social engineering through descriptions they gave of their intentional efforts to build trust as part of the foundation of effective social engineering. A social engineer, Claire, describes how she used the trust of individuals to compromise that organization. She describes spoofing an email from the operations manager of the organization she was attempting to break into to establish a pretext for why she would need access to that organization. She says:

> I used my real name in [the email] just for if they do check government IDs like they're supposed to, they match up. …I walked in and the branch manager walks out of her office before I even say anything to the tellers and names me by name and I'm like, "Oh, I'm screwed." And she was like, "Oh yeah, I just got an email that you were gonna be

> here. It’s so nice to meet you. Blah-blah-blah. What do you need to see?” And led me all around the branch and that happened at all three branches, and they didn’t cover up any of their, they had key codes to get into the private spaces and didn’t cover up when they typed in the key codes. …A lot of it is complacency; people don’t, aren’t suspicious. They just automatically assume I’m supposed to be there and that they don’t double check email, where the email came from or, “Hey, does anybody know who that is,” you know?

In Claire’s retelling of this social engineering engagement, trust is portrayed as a tacit stance taken by people in lieu of any overt aberrant circumstances that they might find difficult to ignore. Due to a lack of appropriate perceptual strategies, targets do not engage in effective cognitive strategies to detect the deception, nor do they engage in behavioral strategies to verify the legitimacy of the social engineer’s presence.

Jeremiah further illustrates the consequences of a lack of effective perceptual strategy in his retelling social engineering engagements he has conducted, in which even technological failures can be overcome by a social engineer when the target of the engagement is trusting. He says:

> …You know, when we do this for clients, you know, I may gain their trust and then something technologically fails…but because I have their trust, I can go back and they’ll come back to me and they’ll have me troubleshoot it with them. And so that’s why the gaining the trust is the success because, you know, if something else fails, they trust you so then you can, you know, keep goin’.

The ability to bypass technological barriers by exploiting trust clearly poses a determent to credulous individuals and the organizations they support. To mitigate against the potential weakness that trust creates regarding social engineering, participants suggested that individuals should engage in a perceptual strategy of skepticism, often expressed in the phrase “trust, but verify[5]” the veracity of communications and narratives that they receive. For participants, the detection of anomalous interactions can occur only when people either do not trust, or verify regardless of trust, the interactions in which they find themselves. Ann describes this dimension of incredulity by saying:

> They are asking for something that, that they shouldn’t have, or that the organization would already know about you. You know, we like tell ‘em your bank doesn’t need your account number – they know it… So they’re asking for something the organization already knows. And, and they’re doing it in a way that just should kind of make your spidey sense tingle…I also tend to emphasize that it’s okay to be rude, you know, give yourself permission to be rude. It’s okay to hang up the phone…You know, you’re, if a legitimate organization is gonna be patient with you while you do that but a scammer is gonna get, gonna get mad and try to pressure you some more.

Social engineering attempts can be detected through instituting policies that require verification and training individuals to feel comfortable in taking the time to verify the authenticity of communications and thereby have a means of detecting potential anomalies. Detecting anomalies, even given the time to conduct verification, often requires an individual to make a determination that hinges on being knowledgeable regarding key factors related to social engineering, as well as cognitively evaluating the interaction for signs of deception. Both strategies will be detailed in the following sections.

Cognitive strategies

Once an appropriate percentual strategy was in place, one method used for the detection of anomalies in social engineering deceptions was described by participants as the result of

[5] This phrase is used more widely than the context of information security. It entered into common parlance in the United States as a result of its usage by Ronald Reagan, who purportedly was taught it as the translation of a Russian proverb ‘doveryai no proveryai.’ (Massie, 2013).

cognitive processes implemented by a targeted individual as these interactions were in the process of occurring. These cognitive strategies were often described by participants through the use of the term "critical thinking." Critical thinking appears to be an umbrella term used by participants to capture a range of non-specific cognitive strategies used in deception detection. The nebulous 'black-box' of critical thinking to detect deception is overtly acknowledged by some participants. In one interview, Anna exemplifies this difficulty in parsing out what critical thinking entails, as she discusses this cognitive process at some length:

> Critical thinking is a….hmm….I kind of love and hate the term because it's gotten a lot of overuse, and a lot of people, if you don't know how to think critically then you don't know how to think critically, so the advice is useless, but it really does come down to what is it that makes sense? So if you're getting a call from someone that says they need something immediately and it's information that you wouldn't normally give out, you shouldn't do it. And, it's a really difficult, it's difficult to teach because the best malicious attackers really do have a way of coming in under the radar. They may not trigger those alarms, you know, they may not make you really mad. They may just make you like 'em a lot. So that's still a strong emotional reaction, I guess, if you meet someone and you like them a lot and you find yourself really wanting to help them. Well, just think about that for a second and think about whether or not that makes sense. So I guess that is sort of the bottom line.

Anna suggests that critical thinking is both necessary for detecting social engineering deceptions, but also paints critical thinking as a cognitive activity that some individuals lack. Moreover, critical thinking is described as somewhat ineffable and innate, as those who lack it cannot be simply instructed in how to engage in it. Despite the lack of clarity surrounding critical thinking, Anna, alongside other participants, illustrates that this cognitive strategy involves a targeted individual engaging in active evaluation and reflection about potentially deceptive situations, rather than allowing the social engineer to pacify them through implications of urgency or the creation of strong emotional states.

Participants highlighted that critical thinking as a cognitive strategy provides agency to targeted individuals because it allows them to contend against the psychological pressures that social engineers will create in interactions, such as creating a sense of urgency or by exploiting strong emotional states. Lucy emphasizes that social engineers intentionally use the creation of urgency in interactions to prevent the opportunity for the other person in the interaction to have time to employ cognitive strategies within the interaction :

> If somebody, especially if you feel like someone is pressuring you, "Why, you know, why do you need my answer right now?" That happens a lot with phone calls or in sales situations sometimes. They'll do the, "Well, this offer's gonna expire." And in social engineering, we always have this urgency to things 'cause we want you off balance and we want you to not spend a lot of time thinking it through, so we want you to just do, click, give me the password, whatever.

Gus explicitly evokes the need for critical thinking when attempting to detect social engineering deceptions in situations involving strong emotions. He says, "So if you get an email that makes you really mad or excited to respond immediately, or if you get a request in person or over the phone that goes something in that way, I think that the thing that we stress above all is just take a little bit of time to think critically about this request and think about whether or not it makes sense." Critical thinking in this context involves carving out time within an interaction and then utilizing that time to evaluate the interaction—a move that creates space to a target of deception to take an agentic role within the interaction rather than simply responding passively or automatically to social engineering requests.

The ability of individuals to determine whether or not a given interaction 'makes sense' through the use of cognitive strategies implies that in these interactions may contain anomalies that would not make sense if subjected to cognitive analysis. This sensemaking within these cognitive processes is intertwined with the ability to use appropriate knowledge-based strategies to permit the detection of potential anomalies within interactions. The ability to evaluate an interaction or communication for features that could point to deception is bolstered by relevant knowledge about the context surrounding the interaction. The analysis will now turn to an examination of the use of knowledge-based strategies.

Knowledge-based strategies

Knowledge-based strategies were characterized by participants as a framework against social engineering interactions could be evaluated for anomalies that could be indicative of deceptions. The knowledge resources that individuals may draw when employing this strategy to detect social engineering deceptions were categorized as two types by the participants. First, participants described the importance of knowing how systems, processes, organizations, or institutions functioned, which would provide a knowledge basis that targets would then be able to use to ascertain if communications from social engineers seemed anomalous to typical communications. Specific aspects of this knowledge were described as intentionally taught to individuals, through trainings or policies, to allow them to be able to detect deceptions should they occur. Second, participants highlighted the importance of knowledge regarding the ways that particular facts, or sets of facts, could be exploited by social engineers. The role of knowledge-based strategies in each of these cases will be elucidated in turn.

Knowledge about internal organization policies was used by participants as an example of the type of knowledge that could allow social engineering to be detected. Cassie discussed a security awareness campaign of consistently messaging that the IT department would never request credentials from their users over email and then offered an example of testing whether employees would follow the guidance from the IT department, saying:

> …That's the number one thing. We will never ask for your credentials…The vice president for finance and administration got a phish from me…it looked so real, and he knew, of course, 'cause he knew what I was askin' for, I would never ask him over email because that's what I say. And he sent it to me and he was like, "Hey, look. This is not you, right?"

The vice president's knowledge that there was an organizational policy against sending credentials over email allowed for the deceptive phishing attempt to be detected. In addition to knowledge regarding specific policies, knowledge about broader aspects of society was also seen as helpful in detecting anomalies that could indicate a social engineering deception. Marilyn sketched out an example of how this broader knowledge could be employed in a discussion of identifying phone scams. She said:

> …I got a phone call that I'm like, "Oh, this is a scam," because it not only has my same area code, it has the first three digits of my phone number. And like I just know, like I don't know anybody else who has those same six beginning digits of their phone number that I care about. And if they honestly care about me, they will leave me a voice mail. But I think that's something that I learned because the first time it happens, I was like, "Oh, not only is it a local call but like someone has like a phone number very similar to mine, like it's probably someone I know." And, so you answer the phone and immediately you know, "Okay, this is a scam." And, so you learn.

Marilyn's story illustrates the nuances of the role that knowledge can play in deception detection. In her description of the first experience receiving a scam call with the same area code and digits as her own, she answers the call, yet is still able to detect that it is a scam call. However, her additional knowledge allows for evaluation of the phone number that now enables her to detect the likely deception prior to initiating communication with the would-be scammers. Employing a knowledge-based strategy, in this case, allows for the detection of potential deceptions with more alacrity, but does not serve as the only sufficient condition for detecting anomalies.

Knowledge regarding how information can be used by social engineers was also seen by participants as a means of evading or detecting potential deceptions. One form of this knowledge was the knowledge of contexts and the varying likelihoods that a deception was occurring across those contexts. Patrick parsed out this distinction in discussing giving over sensitive information in two situations. He said:

> If I'm calling my mortgage company and I got the number from my statement that I got or, you know, like I have it from a pretty secure source, that I know this is the right number, and I phone them and they ask me for the last four digits of my social, right? Then I'm authenticating to them and that's fine, and that's a legit transaction. But if somebody calls me and says, "I'm from x-y-z mortgage company, can I authenticate you, could you please give me the last four digits of your social?" Then I'm not inclined to do that because I have no way of vetting the other side, right?

For Patrick, knowledge of the conditions under which it is an authentic part of the mortgage institution's process to request a social security number allows him to evaluate the context in terms of its potential for being a deception. While the sensitivity of the information provided is the same in both scenarios, the context of providing the information differs, and the knowledge of appropriate context to provide this information serves as the ground for evaluating the potential for deception.

In addition to contexts, the knowledge regarding the availability of information was identified as another factor that is relevant in detecting deceptions. More specifically, participants discussed the importance of knowing the audience that could be accessing potentially important information. One situation in which this sort of knowledge was important for determining if a deception could be occurring was elaborated on by Joan, who said:

> My best advice would be don't ever allow anyone to authenticate with you on something that is publicly available. So, if you have pictures of yourself, and your family, and your friends, if somebody says like, "Oh, yeah. Your cousin, Sarah, told me to give you a call. She said that your dog was sick." If all that's on Facebook or Twitter, you can't allow yourself to be verified with who they are based on that information.

Knowledge about how sets of facts can be exploited by social engineers was also seen as allowing individuals to detect deceptions or foil the intended goal of the deception. This dimension of knowledge is highlighted by Ida who said:

> I was at a police station, actually, the other day, and somebody, somebody came up while I was in the police station and said, "Hi, I'm here for a meeting with the detective, but I can't remember what their name is. Would you read off the list of detectives for me?" And that, that was kind of, I, my ears were burning because I knew that that was sensitive information, and I was a little bit worried that she was, that the receptionist behind the desk was gonna hand it over… But she didn't. She was like, "No, if you have a meeting with a detective then just give me your name and I'll let the detectives know when you get here." And that was the perfect response…that was very impressive to me because you don't see that a lot kind of in the wild, that sort of awareness, and the knowledge of what that information could be used for.

Although Ida frames the receptionist's response as resulting from knowledge and awareness of the value of the information that was being requested, it is also possible that departmental policies and trainings played a role in the fact that the reception declined to provide the information. In this way, knowledge can work in tandem with polices and trainings to allow individuals to detect or evade deceptions.

Reliance on knowledge of the types of facts that social engineers can exploit may be a challenging task, as social engineers can put a disparate array of seemingly innocuous details to use. Patrick laid out this process through describing his social engineering information collection strategies:

> …Even small pieces of information when pieced together can suddenly become harmful. ….For example, if I know, one of the things I found out about [a company] was who does their cleaning service, and because they had a, the cleaning service had a quote on their webpage that they'd be working for this landlord for 30 years, and then they also had pictures of their employees online that showed what the uniform looked like, right? …Now I know how I need to dress to walk into the building without getting asked a question, right? Every bit of information in that chain is pretty meaningless, you know, what color t-shirt I wear and, you know, who cares? But all of that taken together is actually pretty powerful. So, also be careful with the small pieces of information.

While knowledge may serve individuals in being able to detect certain deceptions, it appears to hardly be an ironclad mechanism for detecting all deceptions. Individuals may not be able to determine the full context in which social engineers intend to use a range of information, nor may they know the extent to which social engineers have gathered seemingly private information that adds legitimacy to the deceptive pretexts. On the other hand, the utilization of knowledge-based strategies also bolsters the ability of individuals to detect deceptions, especially when the knowledge is implemented alongside compliance with policies designed to prevent social engineers from being successful in their deceptions.

Aspects of the detection of deception were attributed individualized characteristics, especially with regards to utilizing cognitive strategies in contending against deceptions that were designed to produce emotional intensity, the need to not trust, but rather to employ perceptual strategies to verify potentially deceptive communications, and the use of knowledge-based strategies to detect anomalous aspects of communication. Another dimension of detecting deceptions in social engineering interactions described by participants, however, entailed the externalization of detection of deceptions, rather than relying on each individual to independently be able to determine when such deceptions were occurring. This externalization of deception detection is now examined.

Externalized anomaly detection

Externalized deception detection strategies do not place the onus of deception detection on targeted individuals, but rather seek to shunt the evaluation of potential deceptions to entities with the capability to effectively evaluate deception. These externalized strategies fell broadly into two categories. First, participants describe the designation of knowledgeable parties, such as individuals, departments with an organization, or external vendors to assess potential deceptions. Second, participants described the automation of deception detection through the implementation of technical controls to detect and screen out potential deceptions, or by sending anomaly cues to indicate that a deception might be occurring. Regardless of the particulars of the strategy, this externalized form of deception detection was characterized by the efforts to mitigate, or remove, of the obligation of individuals who were potential targets of social engineering from having to determine whether the interaction was deceptive.

Outsourcing strategies

The external evaluation of potential social engineering deceptions was characterized by participants as important for individuals who were targeted by social engineering deceptions, but who lacked the critical thinking, or incredulity, required to adequately detect anomalies in these interactions. Anna demonstrated this perception of the outsourcing of deception detection while discussing her approach to protecting her own mother from social engineering scams. Anna said of these interactions with her mom, "She's not tech savvy… I have kind of drawn a line with her and said, you know, 'If you get an email from someone that you don't know. Don't just, just don't even respond to it. And if you get an email even from somebody that you know, that asks you to click on something, don't click on that either - just call me.'" Instead of relying on training or education as a method of bolstering her mother's deception detection abilities, Anna asks that potentially deceptive messages be relayed to her so that she can be the knowledgeable party to evaluate that message.

Another reason that participants emphasized as important in allowing another knowledgeable person to evaluate the potential deception was that it would allow the response to a deception be escalated, as the deception is not simply targeted at one individual, but across a range of individuals within an organization. Participants who took this standpoint, often focused on the assistance that individuals within the organization were providing to overall organizational security, rather than framing the need to have a knowledgeable person evaluate the communication as due to any individual deficiency. Dorian provided such an example, and focused on the way in which encouraging the outsourcing of deception detection promoted a culture of organizational security. He said:

> I know on the network side, you know, the people who are most successful in that are the guys who, you know, they, any time, they tell ‘em, “Any time someone sees a suspicious email forward it to us and let us know,” and then they say, “We make sure that every time one of those emails come in,” even if it’s completely benign, you know, we kind of add a little message like, “Hey, thanks for sending this and, you know, we looked at it and, you know, here’s, this is why this one’s not bad. But, you know, thanks for sending it to us. Thanks for keepin’ an eye out.” And, you know, it makes them, and it’s not so much as an us versus them, it makes them part of the security teach, and part of the, you know, the effort to protect the company.

In this framing of the role of the individual in deception detection with an organization, there is not an expectation that the person would, or should, be able to correctly evaluate a message for deception. Rather, the security role for individuals within the organization is to convey potentially deceptive messages to the designated department of knowledge individuals with the expertise to evaluate such messages. The coordination between the various roles of the individuals within the organization is described as promoting security, but without placing the burden of deception detection on all individuals within the organization.

Deception detection was also characterized as being outsourced more broadly across the organization. One information security professional, Doris, gave an example of her organization's response to deception detection that relied on individuals relaying potentially deceptive messages to the information security team. She elaborated by saying:

> …One of the things we do to mitigate that is as soon as somebody reports a scam coming through like a phishing, an email, then we immediately delete that email message from other boxes. So we have, you know, our internal operations, you know, they send scripts so then they pull out all those emails so that nobody else clicks on them. So we rely on that first detector to report that there's a problem.

This procedure essentially crowdsources deception detection, as a multitude of individuals in the organization are exposed to the potentially deceptive message, any one of whom might forward it to the operations team to prevent others from reading the emails. In this case, deception detection is outsourced across the organization as a whole, and individuals who are less sensitive to detecting anomalies that could indicate deception are protected from those messages once they are detected and removed. David gave an example of this approach to deception detection within his organization, saying: "…if you're sending thousands and thousands of emails, some of 'em will go through the filter and some of the individuals afterwards, before the communication goes out about it, five or six of the individuals already have clicked on it."

In this understanding of outsourcing deception detection, there are a broader range of knowledgeable individuals who are tasked with the evaluation of deceptive messages, yet the burden of the evaluation of such messages is removed from individuals who might lack the capacity to correctly identify them as deceptive.

Automation detection strategies

Automated anomaly detection strategies were also described as an organizational process that could aid in the detection of social engineering deceptions and alleviate the necessity of individuals to detect such deceptions. This form of anomaly detection is a technical control that tended to be purchased and implemented through a vendor, such as an email service provider. Harriet's discussion of these automated controls exemplified a typical swath of these technologies with an organization, as she said, "…We have firewalls in place, you know, for people that are just out phishing … We also have email filters that try to kind of grab those emails that look suspicious before they even get to a user. And then we do have anti-virus software on the PCs." This form of deception detection occurs through technological measures, without having to be directly evaluated by a human.

Perhaps counterintuitively, the crowdsourcing aspect of deception detection remains in automated deception detection, as the technology vendor collects information across organizations to evaluate the dynamic threat landscape and update their technology. Roger discusses this component of automated deception detection using the primary example used by participants of automated anomaly detection: the use of email filters to detect phishing emails and prevent these emails from landing in the inboxes of users. He said:

> …The email gateway providers are pretty good at filtering out ninety nine percent of the crap because they just have, they build model, artificial intelligence, and because they sit so many places, they see a lot of it, you know, they may get through to one guy but then by the time they come to your company, hopefully, hopefully you're not the first victim, right?

The use of technical tools outsources the deception detection beyond an individual organization and places vendors in the place of knowledgeable individuals, who specialize in evaluating potential deceptions and who, through technical controls, detect anomalous communications prior to a potentially vulnerable individual receiving such messages.

Participants who discussed automated deception detection often described it as the first line of defense to mitigate the need for individual anomaly detection to occur. An aspect of automated deception detection that was highlighted by participants as a limiting factor of this form of deception detection, however, was the cost associated with acquiring the tools necessary for its implementation. Cassie discussed this challenge for automated deception detection in her work at a university, saying:

> What we need is a better email tool so that students' email accounts, we can stop the phishing. So we've got to buy some software for that. Right now, we don't have the money to do it….So I have, my sister is actually taking classes here, and she said, "Look at my email." And her email was about 80 percent phishing, and I'm not kidding.

For those participants who had invested in automated deception detection, the tools were often characterized as a useful method of reducing the quantity of deceptive communications that individuals were tasked with evaluating. A technology executive in a large organization framed automated deception detection in this way: "The amount of email that don't get to our boxes is 10,000-plus a day, that come in that our various filters kill before they ever go out…some are just spam but are socially engineered attacks. You know, so it's a combination of that and you constantly have to educate people."

The linkage of education and training to automated forms of deception detection was also made by Cassius, who stated, "I would spend money on makin' sure you had a good filter in place, I would spend money on what I'm spending money on, and I would, I would do even a better job of the training aspect of what we're doing." The connection between automated deception detection and the education of individuals underscores that automated deception detection is an imperfect means of capturing all deceptions directed towards individuals. While automating deception detection could ease the burden placed on individuals, without education and training on organizational policies, individuals could still fail to correctly evaluate deceptive communications. Andrea discussed the limitations of automated anomaly detection in her discussion of her organization. She said:

> So we have lots of filtering, it just doesn't catch it all… And it's gotten worse. We would hope it's gotten better but it's gotten worse. The scams and the ability to get through our filters…People pull out of their junk folder and respond. So we make sure it goes to their junk folder, and then they look, and then they think, "Oh, I missed that." And then they respond to that.

While automated deception detection alleviates the quantity of evaluations that individuals have to do, once an individual receives the communication, they have to rely on their trainings and policy compliance to appropriately respond.

Training was also used alongside automated deception detection methods, such as training users to be cautious of warnings that a message could be dangerous. Jerry described this type of training in the context of phishing:

> So we take phishing is a big, right now, it is the number one threat factor that we see in our clients.…we have training that we offer to our clients around it as well. You know, how to spot those things. The technology that gets put into place to help give warnings about it. We do things like our email gateway, well, if it's from an external party, regardless of who it says it is, there's a tag in the front of it that gets, that gets put on the subject of the email. So we teach them things like how to spot that…

The role of automated warnings serves a different purpose than automation designed to prevent deceptive messages from reaching individuals. These automated warnings, instead, are meant to cue individuals into a more skeptical posture and prevent them from unreflectively accepting the content of potentially deceptive messages.

The automation of deception detection, the outsourcing of deception detection to knowledgeable parties, and the ability of individuals to detect anomalies indicative of deception, are all characterized as important dimensions of deception detection. The extent to which each of these components were framed as interacting with one another varied across participants. For some, deception detection relied heavily on individual cognition and knowledge, while the role of knowledge individuals, such as individuals in IT departments, was also emphasized by others. Automated deception detection additionally provided a buffer against individuals being bombarded with mendacious messages, as well as provides a signal around information that should not be trusted.

Discussion

The results indicate that deception detection in social engineering interactions was framed as occurring through individualized strategies that would allow a person to detect anomalies that revealed deception, which consisted of perceptual strategies, cognitive strategies, and knowledge-based strategies. Deception in social engineering interactions could also be detected through externalized strategies through outsourcing anomaly detection to others; either individuals who had the necessary evaluation skills, organizational departments and external vendors specifically tasked with deception detection, or technologies designed to detect deceptions.

The finding that participants accentuated the importance using perceptual strategies that promote skepticism in encounters that could be potentially deceptive points to a recognition of the phenomenon of truth bias as impacting individuals' ability to detect deceptions. Truth bias, or the inclination of people to believe, rather than disbelieve communications from others, has been attributed as one factor that impacts successful deception detection (Buller and Burgoon, 1996;

Stewart, Wright & Atherton, 2019; Van Swol, Braun, & Kolb, 2015). In recommending that individuals employ perceptual strategies that assume that an interaction or communication could be deceptive, participants seem to be suggesting a strategy to contend against truth bias. Thus, when participants, such as Anna, assert that people who receive potentially deceptive communications should "…think about whether or not that makes sense," an assumption is implied that incredulity and cognition can reveal anomalies and cause the detection of deceptions. However, this emphasis on evaluating communications provides no way of accounting for investigator bias[6], which suggests that individuals can be primed to suspect that deceptions are occurring, but that the accuracy of these detections is not improved (Meissner & Kassin, 2002). In investigator bias, individuals have an increased sensitivity to the potential of deception, but tend to not have improved discernment about what communications are, in fact, conveying deception; creating an increase in false positives in the efforts to detect deception, as behavioral cues used to detect deceptions are often inaccurate (Levine and McCornack, 2014).

The findings that the cognitive strategies are imputed as an important component of deception detection is reflected in the focus of much of the literature on deception detection, which tends to frame the detection of deception as something that an individual does through perception or cognition (Buller & Burgoon, 1996; Depaulo, Ansfield, & Bell, 1996; Levine & McCornack, 1991; Park, et al., 2002). As other literature within the body of work on the topic shows, however, the extent to which individuals can make accurate determinations regarding deceptions is ambiguous, and often found to be no higher than the rate of deception detection that could be attributable to chance (Bond & DePaulo, 2006; Burgoon, Buller, Levine &

[6] Sometimes also referred to as 'lie bias' (Kim & Levine, 2011).

McCornack, 2014; Wright, Berry & Bird, 2012). The results of this analysis mirror the ambiguity expressed in the detection deception research, as the participants collectively express a range of views as to the detection abilities of some, or all, individuals.

Individual cognition and disposition to trust are thereby shown to be a necessary, but not sufficient, component of deception detection. For an anomaly to be detected, individuals must be willing and able to evaluate interactions for anomalies that could indicate deceptions. At the same time, however, the anomalies that individuals suspect as pointing to deception may not be accurate signals of real deception.

Knowledge-based strategies can equip individuals to detect deceptions more accurately in social engineering encounters. The analysis identified two categories of knowledge that can contribute to deception detection. These were knowledge of policies or practices within organizations and knowledge of the strategies and information that social engineers exploit in the process of social engineering. The significance of knowledge has also been examined by a narrow strand of deception detection literature (Blair, Levine, & Shaw, 2010; Kim & Levine, 2011; Park et al., 2002). Blair, Levine and Shaw (2010) propose that there are three types of knowledge that are of relevance for deception detection: knowledge that contradicts particular assertions, normative knowledge about standard practices, routine activities, or individual behavior, and 'idiosyncratic information,' which is information that can be used as circumstantial evidence against a deceptive assertion.

The analysis reflects the implementation of knowledge in these categories in the use of deception detection. For example, Wesley points to the utilization of normative knowledge in saying "You need to know your audience. You know you who you get emails from, you know your vendors, anything that seems odd is more than likely an attempt…" Zeke experiences his own deception being detected through knowledge directly contradicts his assertions when he claims to be “Bob Smith” to someone who actually knows the real Bob Smith.

While individuals can draw on knowledge resources to definitively disprove a fabrication and reveal deceptions, the reality of everyday interactions more often entails that individuals might draw upon knowledge resources and become suspicious that an interaction might be deceptive, rather than convinced that it is such. The results indicate a proposed solution to this situation, in the form of authenticating the communications being received, which is the seeking out of dispositive evidence to contradict or confirm the potential deception. Participants suggested methods of verifying the legitimacy of potential deceptions in a variety of manners, often contingent on communication medium. Several participants suggested calling already known phone numbers of vendors to verify whether unexpected emails soliciting payments or changes to accounts were genuine. Patrick suggested authenticating tailgaters in saying, “if somebody is walking in the door with you and tailgating you, even if you’ve had like a five-minute conversation outside…then you should ask ‘em, “Hey, I’m sorry, we’ve just met, can you just swipe your badge?” The success or failure of the badge swipe provides evidence as to the authentic authorization that the person may have to the building.

While authentication may amplify the ability of individuals to detect deception, it can also aid social engineers in solidifying the veneer of the veracity of their deceptions if they are able to fabricate authentication. In *Frame Analysis*, Goffman (1974) notes this consequence of authentication, stating:

> When an individual…comes wonder whether or not he has mistaken the primary framework or key or is being duped or deluded, he seeks for confirmatory evidence. The more he suspects his situation, the more will he seek out bits of evidence he presumes to

> be foolproof. He thus becomes particularly vulnerable to the faking of this evidence, since he will be trustful of it and very dependent on it (Goffman, 1974, p. 463).

A deceiver may employ a wide range of strategies to provide false authentication; they may engage in collusion with a third party who falsely verifies the legitimacy of the deception (Goffman, 1974, p. 84). In elaborate cons, the scammer may build up their deceptions over a series of interactions over time, some of which may incorporate in genuine information that seems to authenticate the legitimacy of the con man. He offers an example of a con man who has arranged access to a private room in a bank, and meets there with victims, presumably to legitimize his financial credentials, saying that the con man has "lifted a genuine scene (and a costly one to fabricate) into his design, the scene being genuine at one level and false at another" (Goffman, 1974, p. 122).

The participants in the present study offered examples of exploiting authentication in the manner described by Goffman (1974). Zeke described a social engineering engagement in which he cloned an employee's badge:

> I saw somebody from this facility that we're trying to go to, walk past, and I went and I bumped into 'em and I cloned their badge right there, right? …And then we went to this facility and I got access. I walked right in, badged right in… security looked at me, I wave at him, he waves at me, keep walkin' through, you know, armed guards, everything, you know, walk right into the building, right?

The ability to clone a badge and authenticate oneself as having legitimate access to a secure location reinforces Zeke's deception, because he has provided confirmatory evidence that he has permission to enter the building. Another example was provided by Claire, who described spoofing an email that impersonated a trusted third party, an organization's operations manager, to provide an authentication for her presence in an office during a social engineering engagement.

The results of the analysis indicate two additional components of the deception detection process that can augment perceptual, cognitive, and knowledge-based strategies to allow deception detection to take place in social engineering encounters: the externalized deception detection strategies of outsourcing detection and automation. Outsourcing deception detection, through automation by asking potential deceptions to be evaluated by knowledgeable parties, encourages all individuals in a group to have high sensitivity to potential anomalies that indicate deception, without relying on those individuals to be able to make accurate determinations as to the veracity of the interaction. Outsourcing deception detection also relies on knowledge, as the knowledgeable parties must themselves be able to accurately identify deceptions. This system may be imperfect, as in the case of automated deception detection of spam emails, which may fail to capture 100% of spam emails. Outsourcing deception detection may also be effective, as reports of potential phishing scams to a knowledge party, such as an IT department, may trigger further investigation leading to evidence that contradicts the message's claim of authenticity and indicates that it is, in fact, social engineering.

The results point to a particular form of outsourcing deception detection, which is a pooled form of deception detection, in which one individual reports a deception that individuals across an organization may have been exposed to, thus potentially preventing susceptible individuals from being deceived. It is this form of deception detection referred to by Doris in her statement that, "…as soon as somebody reports a scam coming through like a phishing, an email, then we immediately delete that email message from other boxes." This strategy of deception detection raises an empirical question: are rates of reliable and accurate deception detection increased when multiple individuals can examine a potential deception?

The deception detection literature has touched on this question, though it has been stated that significant gaps remain in investigation of this topic (Zhou, Zhand, & Sung, 2013). The research in this area tends to focus on the group dynamics of potential deceivers, such as multiple suspects in a criminal investigation (Vernham, Granhag, & Giolla, 2016), rather than the examination of multiple targets of deception. Research that has examined the targets of deception includes a study on deception detection in an online game, which looked at how factors such as group diversity, impacted the success of deception detection (Zhou, Zhand, & Sung, 2013). Most of the remaining studies in this area examined how small groups of 2 to 3 people compared to individuals in scenarios of watching video clips of true or false statements. Of these studies, one found that groups were not more accurate in deception detection than individuals (Park, Levine, Harms, Ferrara, 2002). Building on this study, McHaney, George, and Gupta (2018) found that while groups created by the researchers specifically for the study did not outperform individuals in deception detection, groups that had been priorly established had significantly higher rates of deception detection accuracy in this task. Lastly, a study additionally found that while small groups outperformed individuals in deception detection, this effect was accounted for by the number of people in the small groups with attachment anxiety (Tsachi, Perry-Paldi, Daniely, Zohar-Cohen, & Hirschberger, 2016). The sparsity of research in the area of deception detection across large groups, and the absence of such research in the area of social engineering and phishing scams in particular, points to the need for future research in this area.

The analysis also revealed an aspect of outsourcing deception detection that is specifically characteristic of social engineering deceptions that take place over technological forms of communication: automated deception detection. The automation of deception detection has been a point of focus in the social engineering literature, which has examined how the detection of deception can be automated across a wide range of communication technologies, including social media platforms (e.g. van der Walt, Eloff, & Grobler, 2018), spam phone calls (e.g. Azad, Alazab Riaz, Arshad, & Abullah, 2020), and across emails (e.g. Ludwig, Van Laer, Ruyter, Friedman, 2016; Sheikhalishahi, Saracino, Martinelli, La Marra, Mejri, & Tawbi, 2020). The field of deception detection, in its consideration of computer mediated communication (CMC), has for the most part overlooked automation and tended, instead, to focus on the cues that individuals use to detect deceptions that occur using CMC, and how successful deception detection is in these contexts (Hancock, Woodworth, & Goorah, 2010; Pak & Zhou, 2014; Tong & Walther, 2015; Van Swol, Braun, & Kolb, 2015).

The automation of deception detection elucidated in the present analysis is contingent upon the technologies that allow mediated communication to occur in the first place. Filtering spam from an email inbox does not happen without the existence of email; screening robocalls relies on the presence and use of telephones, and multi-factor authentication is dependent on a technological system with the ability to authenticate. Given this situation, the question arises, does detection of deception through automated means represent a wholly new form of deception detection that requires information technology as an antecedent?

The results offer some hints towards the answer to this question. The automated systems used to detect social engineering described by the participants appear to automate the same processes that individuals engage in when evaluating interactions for deception. Multi-factor authentication, in which a system requires credentials from two different sources, serves as an automated form of the same type of authentication that Mark suggests people engage in by finding a way to double-check the veracity of callers after asking themselves, “Well, why are they phonin’ me and have I validated their identity?”

The firewalls and filters discussed by Andrea, Cassius, and Harriett also act as an automated process to detect anomalies that indicate deception and prevent these deceptions from reaching their intended targets. In a similar manner, participants described their personal, non-automated anomaly detection and communication filtering processes, such as the description offered by Marylin that "I'm like, "Oh, this is a scam," because it not only has my same area code; it has the first three digits of my phone number."

Automated deception detection has therefore taken a social process and melded it into a partially technological process. Interactional dimensions may remain, as people continue to interact both with each other, and with technological interfaces through these mediated communication and automated deception detection processes. One way to describe this process might be through the inclusion of technology as actors who participate within the social interaction, perhaps as illustrated by Latour's (2005) actor-network-theory. Within this theoretical perspective, technology itself could be framed as a participant that might detect deception, as opposed to a mediator through which a human perceives that deception may be occurring. Alternatively, automated deception detection across CMC may also be represented through Haraway's (1985, p. 69) image of the cyborg, as the distinction between human and machine anomaly detection across interactions becomes increasingly ambiguous. There is some indication that automated deception detection may surpass human deception detection and even be impeded by human evaluations of anomalies (Kleinberg & Verschuere, 2021). This is echoed in Andrea's statement that "So we have lots of filtering, it just doesn't catch it all…People pull out of their junk folder and respond." This situation, in which human interactions through mediated technological communications are evaluated by automated systems, potentially more effectively than human evaluation, could be encompassed by Haraway's (1985, p. 99) evaluation that "The machine is us, our processes, an aspect of our embodiment."

Haraway's (1985) image of the cyborg expands beyond the role automated deception detection in detecting social engineering, to apply more broadly to the structure of society in which social engineering and deception detection are taking place. Under late capitalism, a central point of focus for society is the control of the flow of information across permeable boundaries, with human beings integrated as part of the architecture of this system (Haraway, 1985, p. 82-83). Thus, "One should expect control strategies to concentrate on boundary conditions and interfaces, on rates of flow across boundaries—and not on the integrity of natural objects. 'Integrity' or 'sincerity' of the Western self gives way to decision procedures and expert systems" (Haraway, 1985, p. 81). The context in which deception detection in social engineering interactions occurs can therefore be understood as intertwined within the conditions of modernity, as individuals evaluate whether they can trust the communications of individuals, who are often unknown to them, but who represent themselves as part of the expert systems by which society is structured (Giddens, 1990).

Conclusion

The analysis points to deception detection in social engineering interactions occurring through the detection on anomalies that point to the deceptive character of the interaction. This anomaly detection may be the result of an individual's evaluation of an interaction or the outsourcing of that evaluation to knowledgeable parties or technologies. Regardless of the particulars of the detection of anomalies, participants uniformly indicated that the deception of social engineering was imperfect; this imperfection of deception detection in a wide range of contexts has also been noted within the deception detection literature (Bond & DePaulo, 2006;

Burgoon, Buller, Ebes & Rockwell, 1994; Levine & McCornack, 2014; Wright, Berry & Bird, 2012).

These results have implications for policies, practices, and research that seeks to reduce the impact of social engineering on individuals and organizations. Individuals are embedded within a system in which reliance is placed on expert systems exploited by social engineers and it is of questionable utility to anticipate effective individual response to a systemic issue. Organizations should instead focus on policies and practices that create a robust system in which potential deceptions can be screened automatically and evaluated by knowledgeable parties. Given the difficulty of universal deception detection, organizations should ensure that incident response systems can rapidly respond to mitigate the impact of social engineering deceptions when they successfully occur.

A future research agenda stemming from the results of this study could focus on deception detection at a group or organizational level, rather than the individual level. For example, does having a shared inbox where multiple members of a team can evaluate received emails for potential deceptions increase accurate deception detection? Future research could also examine the extent to which organizational policies and practices may create systems in which individuals are expected or incentive to trust interactions in their everyday work experiences.

Chapter 7 - Conclusion

This section will conclude the dissertation by considering how the three analyses combined may have implications in mitigating against the impacts of social engineering and bolstering the efficacy of security awareness practices. While theoretical and security awareness consequences specific to each of the research questions have already been highlighted in the prior discussion sections of each analysis, the following section will provide a high-level overview of potential ramifications of the findings collectively. There is first a summary of the three research questions and the analyses prior to considering the potential implications of these findings. Limitations of the research project and analyses are then discussed. Lastly, topic areas of relevance for a future research agenda are addressed.

This dissertation examined three aspects of social engineering while keeping at the fore the theoretical importance of social interaction within this phenomenon (McGuire, 2018). Three research questions were analyzed:

1. What are the experiential dimensions of engaging in social engineering?
2. How do social engineers attempt to maintain deceptions while engaging in social engineering?
3. How does deception detection occur in social engineering interactions?

The first two analyses interrogate facets of the interactive elements within the control and experience of the social engineer. The first analysis specifically examines the affective attributes of attempting social engineering; lending insight into potential motivations for social engineering, as well as potential routes to dissuade social engineers. This analysis illustrates the emotional dimensions of the social engineering experience, which ranges from intense excitement to mundane boredom. The analysis then examines the ways in which features of the social engineering interaction can mediate the affective experience of social engineering, Specifically, the results examine the ways in which mediated communication, such as through phone or email, can shape the experience of social engineering perpetration, as can the ways in which social engineers frame their targets. Lastly, the analysis found that the ways in which social engineers understood themselves played a role in their experiences of social engineering.

The second analysis examines how social engineers seek to maintain the deceptive façade throughout a social engineering attempt. The results of this analysis explicate bluff and stealth as deceptive structures within which social engineers attempt to maintain their deceptions. The analysis then examines the ways in which communications technologies can facilitate social engineering deceptions, such as by obscuring the identity of a social engineer, as well as the potential challenges that these technologies pose to social engineering deceptions. The analysis similarly examines the impact of institutional structures and cultural norms as factors that can either be exploited by social engineers or impede the success of a social engineering deception.

The third analysis turns to an examination of ways in which the targets of social engineering may avoid being duped, and instead, come to awareness that a deception is taking place. The results of this analysis identified both individualized and externalized strategies used in deception detection. Individualized strategies require an individual to evaluate and act when confronted with an interaction in which social engineering could be occurring. These individualized deception detection strategies are perceptual strategies, cognitive strategies, and knowledge-based strategies. Externalized strategies divert the evaluation of potential deceptions to a designated responsible entity, who could be a knowledgeable individual or group of individuals, such as an IT department, or an automated technological system for deception detection.

Security awareness

Collectively, these analyses suggest that a security awareness program should ensure that an organization has robust policies and practices in place for authenticating the legitimacy of communications and individuals who interact with the organization. Across the analyses, social engineers are revealed as exploiting trust through impersonating membership in expert systems (Giddens, 1990), utilizing communication technologies to disguise or fake their identities, and employing interpersonal skills to evade detection. Implementing organizational authentication policies with these social engineering factors in mind, could promote resiliency against social engineering.

The importance of security awareness policies, broadly construed, have also been emphasized in the literature as of significant importance (Barber, 2001; Townsend, 2010; Nyamsuren & Choi, 2007; Rabinovitch, 2007; Schaab, Beckers, & Pape, 2017). These works have highlighted that lapses in security awareness can allow people to unwittingly facilitate a social engineer's attempts to bypass technical controls and to acquire credentials, gain access a physical location or technical system, or simply collect information that can later be exploited (Barber, 2001; Dahbur, Bashabsheh, & Bashabsheh, 2017; Hu, Dinev, Hart, & Cooke, 2012; Twitchell, 2009).

Furthermore, trainings to promote staff compliance with organizational policies and practices surrounding authentication procedures may be more effective at stymying social engineering attacks than trainings designed to sharpen individual detection skills. The analyses suggest that authenticating potential social engineering attempts, automating deception detection, or outsourcing detection to knowledgeable parties, may be more effective than attempting to bolster the evaluative skills of all employees. Additionally, it may be unrealistic to expect all employees within an organization to successfully contend against the deceptions posed by a skilled social engineer. Instead, promoting compliance with well-developed organizational security policies may better serve to prevent social engineering compromises.

This suggestion to avoid focusing training on the detection abilities of employees breaks with the literature on security awareness trainings, which often contain efforts to teach employees evaluation methods for security threats, including social engineering (e.g. Bulgurcu, Cavusoglu, & Benbasat, 2010; Farooq, Isoaho, Virtanen & Isoaho, 2015; Rocha Flores & Ekstedt, 2016; Tsohou, Kokolakis, Karyda, & Kiountouzis, 2008). On the other hand, research on individual susceptibility to social engineering indicates that there is a range of susceptibility across individuals that is not consistently associated with individual demographic, personality, or technological proficiency variables (security (e.g. Anwar, He, Ash, Yuan, Li & Xu, 2017; Arachchilage & Love, 2014; Goel, Williams, & Dincelli, 2017; Rocha Flores, Holm, Nohlberg, & Ekstedt, 2015; Verkijika, 2019). This research may provide evidence for the futility of successfully training a broad swathe of employees across an organization to reliably detect social engineering.

Theoretical Implications

Each analysis conducted for this dissertation has its own specific theoretical implications (examined in greater detail in the respective discussion sections). Analyzing the affective experience of social engineering points to potential under-examined motivations for engaging in social engineering, as well as implications for the efficacy of deterring certain social engineers. The results of the analysis of how social engineers maintain deceptions illustrates the exploitation of abstract systems (Giddens, 1990) by social engineers, suggesting that social engineering may be a deeply rooted consequence of modernity. In examining how targets of social engineering engage in deception detection, the results highlight a potential area overlooked by both deception detection researchers and security awareness practitioners—that of deception detection by groups, rather than individuals. Specifically, security awareness programs tend to focus on improving the ability of individuals to identify potential deceptions, such as phishing emails. The deception detection results indicate that it may, in fact, be more effective to train individuals to forward suspicious emails to an IT department, which would allow an alert regarding the phishing scam to be disseminated across an organization. This would allow individuals with better detection abilities to serve as detectors for individuals who were less sensitive to deceptions, rather than expecting all individuals to be readily able to discern deception when exposed to it.

Taken as a whole, this dissertation additionally suggests overarching theoretical implications. It has been noted that social engineering is a subset of con-artistry and deception more broadly (Berti & Rogers, 2002). This dissertation, by centering social engineering in the interactional domain, highlights the ways in which social engineering exploits trust and is characterized by deceptive moves made by the social engineer in interactions with targets of the social engineering attempt.

Focusing on the interactional dimensions of social engineering reveals the depth of these deceptions as both dynamic and complex. The theoretical implication of an interactional approach to social engineering is therefore that there are shifting opportunities for detecting deceptions that may occur across the course of a social engineering interaction, as targets of these deceptions gain or lose trust throughout the interaction in performing anomaly detection strategies, and as social engineers work to maintain the deception and portray themselves or their communications as resembling authentic versions of what they purport to be. Contending against a social engineering attempt should thus be understood as an interactional process, across which there are opportunities for interventions to shift the course of the interaction through the implementation of security policies and practices.

An example of examining social engineering as an interactional process can be illustrated using an emerging Business Email Compromise (BEC) scheme that the FBI's Internet Crime Complaint Center (2021) describes as occurring when scammers compromise the email of an executive and then "request employees to participate in virtual meeting platforms. In those meetings, the fraudster would insert a still picture of the CEO with no audio or a "deep fake" audio through which fraudsters, acting as business executives, would then claim their audio/video was not working properly" (IC3, 2021, p.9). The scammers would then instruct the employee to initiate a wire transfer to the scammer's bank account. The interactional process illustrated in this scheme is dynamic and reveals intervals where effective intervention could prevent the social engineer from being able to maintain the deception and allow the employees to detect that such a deception was occurring. If there was a policy in place to prevent wire transfers from being requested in virtual meeting settings, the BEC could be detected early in the interaction. If there was a policy in place requiring that employees authenticate executive request to transfer money with two forms of communication, such as email and a phone call, the deception could also be detected when the executive was called. While the specifics of such policies may vary, contextualizing social engineering scams as an interactional process provides a framework for determining how such policies may be useful.

This dissertation also suggests a potential adaptation of social disorganization theory as a theoretical approach to analyzing the successful prevention of social engineering scams within organizations. Social disorganization theory is an ecological theory of crime which posits that certain places, typically neighborhoods, are susceptible to higher rates of crime due to a lack of social cohesion and stability, which prevents the community from being able to regulate itself through the use of formal and informal social controls to prevent crime from occurring (Bursik & Grasmick, 1993; Shaw & McKay, 1969). In a similar way, social disorganization theory can be used to explore how certain organizations may be susceptible to higher rates of social engineering due to social disorganization within a company.

Social disorganization theorists (Bursik & Grasmick, 1993; Rose & Clear, 1998) suggest that there are three levels of social control that contribute to the ability of communities to engage in self-regulation to maintain organization. These levels of control may serve as a beneficial framework for examining the occurrence of social engineering within organizations. [7] The first of these levels is the individual, or personal level, in which friends and family contribute to informal social controls such as the fear that an action could lead to the disappointment of these individuals. The second level of control that contributes to social organization occurs at the community level, which consists of day-to-day interactions with informal networks and local organizations and institutions, such as offices, libraries, and schools. The macro level of control occurs through public institutions, which impose formal social controls through mechanisms such as regulation and legislation. From the perspective of social disorganization theory, when all three levels of social control function effectively together, a high level of social organization

[7] While social disorganization theorists have identified a range of factors (residential mobility, economic deprivation, population heterogeneity, etc.) theoretically associated with social disorganization at the neighborhood level (Kubrin & Weitzer, 2003), there is no strong theoretical reason to assume that these factors would be transferable to an examination of social engineering within organizations, and will not be focused on here.

and cohesion is maintained, resulting in a reduction in crime. (Bursik & Grasmick, 1993; Rose & Clear, 1998).

Examining social engineering utilizing these three levels of control specified within social disorganization theory may allow for a delineation of where social disorganization is leading to a lack of organizational ability to engage in self-regulation and mitigate against the occurrence of social engineering attacks. The findings from this dissertation suggest that macro level social factors, such as legislation like HIPPA that dictates requirements around access to confidential information, do impose formal social controls on organizations resulting in some degree of self-regulation within those organizations. Within the context of social engineering, the community level would consist of the organization itself, and the controls would be expressed in the extent to which informal networks within the organization promoted a security culture, in addition to the formal social controls of policies to regulate the organization. Lastly, the personal level would be found in the team in which an individual worked, as well as an individual's personal social connections. At this level, informal social controls could promote the use of perceptual and cognitive strategies to mitigate against the success of social engineering.

Limitations

One primary limitation of the analyses in this dissertation concerns the sample that was utilized. The analyses were conducted using a sample of 54 participants, including social engineers, IT professionals, and security auditors. While efforts were made to recruit participants from a broad range of backgrounds and experiences, there are, no doubt, perspectives that are not fully represented in the interviews that were analyzed. It is entirely possible, therefore, that some of the themes within any given analysis could be under-developed due to the absence of relevant data. For example, in the sample of social engineers, none of the participants engaged in social engineering in the context of organized crime. The size of the sample additionally imposes a limitation on the granularity with which the experience of specific types of participants can be parsed out and analyzed as particular to that group. For example, although several social engineers who were women were included in the sample, there was an insufficient quantity to be able to analyze and compare the experience of women to that of men engaging in social engineering. Lastly, the sample was recruited exclusively from Western, English-speaking countries, primarily the United States. The results of the analyses may therefore substantially diverge from experiences of individuals in other countries.

An additional limitation of these analyses is fundamental to the design of qualitative research conducted with semi-structured interviews on a nonprobability sample of participants, which is that no conclusion can be drawn regarding the significance between associations in the themes elucidated in the results (Corbin & Strauss, 2015). Instead, this form of research is used to delineate abstract concepts and elucidate the meaning-structures within subjective experienced (Berg, 2004). While these analyses cannot, and are not intended to, replace quantitative study of these aspects of social engineering, they can act as a foundation for theory-building by which to structure future quantitative projects.

Future research

While a wide-range of future research could extend and further explore the phenomena investigated within this dissertation, this section is limited to three areas of a future research agenda related to the three analyses of within the dissertation, in addition to an overarching call to an area of future research. First, as an extension of the first research question, examining differences in motivations to engage in social engineering, as well as individual characteristics, across different forms of communication might be of value in determining if organizational policies would benefit from being tailored to differing subsets of social engineers. For example, the goals and methods used by a social engineer spamming thousands of phishing emails could be substantially different than those of a social engineer engaging in an in-person attack against an organization. Second, branching out of the maintenance of deceptions analysis, examining the extent to which expert systems are exploited in the commission of crimes writ large could broaden the theoretical importance of expert systems in criminology as a field. In extending the deception detection analysis, a quantitative test of the efficacy of evaluating deceptions as a group of knowledgeable people, rather than by an individual, could provide evidence for a shift in security awareness trainings and policies.

Lastly, social engineering as a phenomenon would benefit from an increase in research focused on white-collar victimology. While this dissertation lends insight into the strategies used by targets of social engineering to detect deceptions and avoid becoming victims, research examining the characteristics of individuals who are susceptible to social engineering has resulted in contrasting and often contradictory findings, with minimal theoretical frameworks for understanding social engineering victimization (Anwar, He, Ash, Yuan, Li & Xu, 2017; Arachchilage & Love, 2014; Goel, Williams, & Dincelli, 2017; McCormac et al., 2017; Verkijika, 2019). White-collar victimology, while perhaps in its nascent stages as a field (Dodge, 2020), could provide deeper insight into the victims of social engineering.

Chapter 8 - References

Abraham, S., & Chengalur-Smith, I. S. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*, 183–196.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers and Security*, *68*, 160–196.

Anderson, Elijah. (1999). *Code of the Street: Decency, Violence, and the Moral Life of the Inner City*. New York: W. W. Norton & Company.

Antheunis, M.L., Schouten, A.P., Valkenburg, P.M., & Peter, J. (2012). Interactive uncertainty reduction strategies and verbal affection in computer-mediated-communication. *Communication Research, 39*(6), 757-780.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443.

Applegate, S. D. (2009). Social engineering: Hacking the wetware! *Information Security Journal*, *18*(1), 40–46.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312.

Arciuli, J., Mallard, D., & Villar, G. (2010). "Um, i can tell you're lying": Linguistic markers of deception versus truth-telling in speech. *Applied Psycholinguistics*, *31*(3), 397–411.

Aurigemma, S., & Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers and Security*, *66*, 218–234.

Azad, M.A., Alazab, M., Riaz, F., Arshad, J. & Abullah, T. (2020). Socioscope: I know who you are, a robot, human caller or service number. *Future Generation Computer Systems, 105*, 297-307.

Babbie, E.R. (2013). *The basics of social research*. Boston, MA: Cengage Learning.

Barber, R. (2001). Social engineering: A people problem? *Network Security*, (7), 9–11.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61.

Berg, B. L. (2004) *Qualitative research methods for the social sciences.* Boston, MA: Pearson.

Berg, B. L. & Lune, H. (2012). *Qualitative methods for the social sciences.* Boston, MA: Pearson.

Berti, J., & Rogers, M. (2002). Social engineering: The forgotten risk. In H. F. Tipton & M. Krause (Eds.), *Information security management handbook* (4th ed., pp. 51–63).

Blair, J. P., Levine, T. R., & Shaw, A. S. (2010). Content in context improves deception detection accuracy. *Human Communication Research*, *36*(3), 423–442.

Blumer, H. (1998). *Symbolic interactionism: Perspective and method.* Englewood Cliffs, NJ: University of California Press.

Bond, C. F., Omar, A., Pitre, U., Lashley, B. R., Skaggs, L. M., & Kirk, C. T. (1992). Fishy-looking liars: Deception judgment from expectancy violation. *Journal of Personality and Social Psychology*, *63*(6), 969–977.

Bond, C. F., & DePaulo, B. M. (2006). Accuracy of deception judgments. *Personality and Social Psychology Review*, *10*(3), 214–234.

Brody, R. G., Brizzee, W. B., & Cano, L. (2012). Flying under the radar: social engineering. *International Journal of Accounting and Information Management*, *20*(4), 335–347.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, *11*(1), 97–115.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks—A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*, *15*(1), 20–45.

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), 268–289.

Burgoon, J. K., Buller, D. B., Ebesc, A. S., & Rockwell, P. (1994). Interpersonal deception: Accuracy in deception detection. *Communication Monographs*.

Burgoon, J. K., Buller, D. B., White, C. H., Afifi, W., & Buslig, A. L. S. (1999). The role of conversational involvement in deceptive interpersonal interactions. *Personality and Social Psychology Bulletin*, *25*(6), 669–683.

Bursik, R.J. & Grasmick, H.G. (1993). *Neighborhoods and crime: The dimensions of effective community control.* New York, NY: Lexington Books.

Buller, D. B., Strzyzewski, K. D., & Hunsaker, F. G. (1991). Interpersonal deception: The inferiority of conversational participants as deception detectors. *Communication Monographs*, *58*, 25–40.

Campbell, C. C. (2018). Solutions for counteracting human deception in social engineering attacks. *Information Technology & People*. https://doi.org/10.1108/ITP-12-2017-0422

Chan, M. (2003). Corporate espionage and workplace trust/distrust. *Journal of Business Ethics*, *42*(1), 45–58.

Charmaz, K. (2002). Qualitative interviewing and grounded theory analysis. In J. F. Gubrium & J. A. Holstein (Eds.) *Handbook of interview research: Context & method* (pp. 675-694). Thousand Oaks, CA: Sage Publications, Inc.

Charmaz, K. (2014). *Constructing grounded theory.* Thousand Oaks, CA: Sage Publications, Inc.

CBC News. (2018, April 4). MacEwan University loses $11.8 million to scammers in phishing attack. CBC News. Retrieved May 29th, 2019 at https://www.cbc.ca/news/canada/edmonton/macewan-university-recovers-most-of-11-8m-online-phishing-scam-1.4604729

Churchill, S.D. & Wertz, F.J. (2001). An introduction to phenomenological research in psychology: Historical, conceptual, and methodological foundations. In K.J. Schneider, J.F. Bugental & J.F. Pierson (Eds.), *The handbook of humanistic psychology: Leading edges in theory, research, and practice* (247-262). Thousand Oaks, CA: Sage Publications.

Cialdini, R. (2008). *Influence: The psychology of persuasion*. New York: Harper Business.

Corbin, J. & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology, 13*(1), 3-21.

Corbin, J. & Strauss, A. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory.* Thousand Oaks, CA: Sage.

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

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology, 21*(2), 187-204.

Cross, C. (2016). ‘They’re very lonely’: Understanding the fraud victimisation of seniors. *International Journal for Crime, Justice and Social Democracy, 5*(4), 60-75.

Curtis, S. R., Rajivan, P., Jones, D. N., & Gonzalez, C. (2018). Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior*, *87*, 174–182.

Cusack, B., & Adedokun, K. (2018). The impact of personality traits on user’s susceptibility to social engineering attacks. In *Proceedings of the 16th Australian Information Security Management Conference* (pp. 83–89). Perth, Australia: Edith Cowan University.

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

Davenport, R. A. (1837). *Sketches of imposture, deception, and credulity*. London: Thomas Tegg and Son.

Depaulo, B. M., Ansfield Matthew, E., & Bell, Kathy, L. (1996). Deception and paradigms for studying it: A critical appraisal of Buller. *Communication Theory*, *8*, 297–310.

DePaulo, B. M., Kirkendol, S. E., Kashy, D. A., Wyer, M. M., & Epstein, J. A. (1996). Lying in Everyday Life. *Journal of Personality and Social Psychology*, *70*(5), 979–995.

Dhiman, P., Wajid, S. A., & Quraishi, F. F. (2017). A comprehensive study of social engineering - The art of mind hacking. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *2*(6), 543–548.

Dirks, K. T., & Ferrin, D. L. (2001). The role of trust in organizational settings. *Organization Science*, *12*(4), 450–467.

Dodge, M. (2020). A black box warning: The marginalization of white-collar crime victimization. *Journal of White Collar and Corporate Crime, 1*(1), 24-33.

Doocy, J. H., Shichor, D., Sechrest, D. K., & Geis, G. (2008). Telemarketing fraud: Who are the tricksters and what makes them trick? *Security Journal*, *14*(3), 7–26.

Dupont, B., Côté, A.M., Savine, C. & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime, 17,* 129-151.

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

Ekman, P. & Friesen, W.V. (1969). Nonverbal leakage and clues to deception. *Psychiatry Journal for the Study of Interpersonal Processes, 32*(1), 88-106.

Esterberg, K. (2002). *Qualitative Methods in Social Research.* McGraw-Hill.

Etzioni, A. (2019). Cyber trust. *Journal of Business Ethics, 156*, 1-13.

Evans, J. R., Michael, S. W., Meissner, C. A., & Brandon, S. E. (2013). Validating a new assessment method for deception detection: Introducing a psychologically based credibility assessment tool. *Journal of Applied Research in Memory and Cognition*, *2*(1), 33–41.

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Observations on genderwise differences among university students in information security awareness. *International Journal of Information Security and Privacy*, *9*(2).

Federal Information Security Management Act, 44 U.S.C. § 3541 (2002).

Ferrell, J. (2004). Boredom, crime and criminology. *Theoretical Criminology*, *8*(3), 287–302.

Ferrell, J., Hayward, K. & Young, J. (2008). *Cultural Criminology: An invitation*. London, UK: Sage.

Frank, M. G., Menasco, M. A., & O'Sullivan, M. (2008). Human behavior and deception detection. In *Handbook of Science and Technology for Homeland Security* (Vol. 5). John Wiley & Sons, Inc.

Forbes. (2019, September 6). Toyota parts supplier hit by $37 million email scam. Forbes. Retrieved February 2, 2022 at https://www.forbes.com/sites/leemathews/2019/09/06/toyota-parts-supplier-hit-by-37-million-email-scam/?sh=396e83565856

Forgas, J. P., & East, R. (2008). On being happy and gullible: Mood effects on skepticism and the detection of deception. *Journal of Experimental Social Psychology*, *44*(5), 1362–1367.

George, J. F., Giordano, G., & Tilley, P. A. (2016). Website credibility and deceiver credibility: Expanding Prominence-Interpretation Theory. *Computers in Human Behavior*, *54*, 83–93.

Gendlin, E. (1997). *Experiencing and the creation of meaning: A philosophical and psychological approach to the subjective.* Evanston, IL: Northwestern University Press.

Giddens, A. (1990). *The consequences of modernity*. Palo Alto, CA: Stanford University Press.

Gillespie, A. A. (2017). The electronic Spanish Prisoner: Romance frauds on the internet. *The Journal of Criminal Law*, *81*(3), 217–231.

Glas, G. (2017). Dimensions of the self in emotion and psychopathology: Consequences for self-management in anxiety and depression. *Philosophy, Psychiatry and Psychology, 24*(2), 143–155.

Glaser, B. G. & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research.* Chicago, IL: Aldine Publishing Company.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1), 22–44.

Goffman, E. (1956). *The presentation of self in everyday life.* New York, NY: Anchor Books.

Goffman, E. (1967). *Interaction ritual*. New York, NY: Double Day, p. 5-45.

Goffman, E. (1974). *Frame analysis: An essay on the organization of experience.* Cambridge, MA: Harvard University Press.

Granhag, P. A., & Strömwall, L. A. (2000). Effects of preconceptions on deception detection and new answers to why lie-catchers often fail. *Psychology, Crime and Law*, *6*(3), 197–218.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of internet fraud: An empirical investigation of deception and trust with experienced internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics*, *30*(4), 395–410.

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Indianapolis, IN: Wiley, Publishing.

Hamlin, I., Wright, G. R. T., Van der Zee, S., & Wilson, S. (2018). The dimensions of deception detection: Self-reported deception cue use is underpinned by two broad factors. *Applied Cognitive Psychology*, *32*(3), 307–314.

Hancock, B. (1995). Simple social engineering. *Network Security*, (6), 13–14.

Hancock, J. T. (2012). Digital deception: Why, when and how people lie online. In *Oxford Handbook of Internet Psychology* (pp. 287–301).

Hancock, J. T., Woodworth, M. T., & Goorha, S. (2010). See no evil: The effect of communication medium and motivation on deception detection. *Group Decision and Negotiation*, *19*(4), 327–343.

Haraway, D. (1985), A manifesto for cyborgs: Science, technology, and socialist feminism in the 1980s. *Socialist Review, 80*, 65-107.

Hauch, V., Sporer, S. L., Michael, S. W., & Meissner, C. A. (2014). Does training improve the detection of deception? A meta-analysis. *Communication Research*, *43*(3), 283–343.

Higgins, B. (Producer), & Morris, F. (Director). (2022) The Tinder Swindler [Video file]. Retrieved on February 3, 2022 from https://www.netflix.com

Hochschild, A.R. (1983). *The managed heart: Commercialization of human feeling*. Berkeley, CA: University of California Press.

Holt, T. & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*(1), 33-50.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660.

Huang, W., & Brockman, A. (2011). Social engineering exploitations in online communications: Examining persuasions used in fraudulent E-mails. In T. J. Holt (Ed.), *Crime online: correlates, causes, and context* (pp. 87–111). Durham, NC: Carolina Academic Press.

Husserl, E. (1983/1913). *Ideas pertaining to a pure phenomenology and to a phenomenological philosophy: First Book*. (F. Kersten, Trans.), New York, NY: Springer.

IC3, Internet Crime Complaint Center, Federal Bureau of Investigation. (2021). *2021 Internet crime report*. Federal Bureau of Investigation. Retrieved March 31, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

IRS. (2019, May 17). Tax scams / consumer alerts. Retrieved May 30, 2019, from https://www.irs.gov/newsroom/tax-scams-consumer-alerts

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.

Ivaturi, K., & Janczewski, L. (2011). A taxonomy for social engineering attacks. In *International Conference on Information Resources Management (CONF-IRM)*.

Jackson, J. E. (1994). Fraud masters: Professional credit card offenders and crime. *Criminal Justice Review*, *19*(1), 24–55.

Jones, K. (1996). Trust as an affective attitude. *Ethics*, *107*(1), 4–25.

Kashian, N. Jang, J. Shin, S.Y. Dai, Y. & Walther, J.B. (2017). Self-disclosure and liking in computer-mediated communication. *Computers in Human Behavior, 71*, 275-283.

Katz, J. (1988). *Seductions of Crime: Moral and Sensual Attractions in Doing Evil.* Basic Books.

Katz, J (2001a). A theory of qualitative methodology: The social system of analytic fieldwork, in *Contemporary Field Research: A Collection of Readings* (ed. Robert Emerson), 127-148.

Katz, J (2001). From how to why: On luminous description and causal inference in ethnography (Part I)," *Ethnography*, *2*(4), 443-473.

Kim, R. K., & Levine, T. R. (2011). The effect of suspicion on deception detection accuracy: optimal level or opposing effects? *Communication Reports*, *24*(2), 51–62.

Kleinberg, B. Verschuere, B., 2021. How humans impair automated deception detection performance. *Acta Psychologica, 213*, 1-9.

Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The role of love stories in romance scams: A qualitative analysis of fraudulent profiles. *International Journal of Cyber Criminology*, *9*(2), 205–217.

Kubrin, C. E., & Weitzer, R. (2003). New directions in social disorganization theory. *Journal of Research in Crime and Delinquency*, *40*(4), 374–402.

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology*, *50*(1), 569–598.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. In *Communications of the ACM* (Vol. 50, pp. 94–100).

Jain, A., Tailang, H., Goswami, H., Dutta, S., Sankhla, M. S., & Kumar, R. (2016). Social engineering: Hacking a human being through technology. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *18*(5), 94–100.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122.

Landry, D. (2013). Are we human? Edgework in defiance of the mundane and measurable. *Critical Criminology, 21*(1), 1–14

Latour, B. (2005). *Reassembling the social: An introduction to Actor-Network-Theory*. New York, NY: Oxford University Press.

Lawson, P. Zielinska, O. Pearson, C. & Mayhorn, C.B. (2017). Interaction of personality and persuasion tactics in email phishing attacks. *Proceedings of the Human Factors and Ergonomics Society 2017 Annual Meeting*, 1331-1333.

Leal, S., Vrij, A. Deeb, H. Hudson, C. Capuozzo, P. & Fisher, R.P. (2020). Verbal cues to deceit when lying through omitting information. *Legal and Criminological Psychology*, 25(2), 278-294.

Leukfeldt, R. Kleemans, E., Stole, W. (2017). The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist, 61*(11), 1387-1402.

Lee, C.J. & Andrade, E.B. (2015). Fear, excitement, and financial risk-taking. *Cognition and Emotion,* 29(1), 178-187.

Levine, T. R. (2010). A few transparent liars explaining 54% accuracy in deception detection experiments. *Annals of the International Communication Association*, *34*(1), 41–61.

Levine, T. R. (2014). Active deception detection. *Policy Insights from the Behavioral and Brain Sciences*, *1*(1), 122–128.

Levine, T. R., Feeley, T. H., McCornack, S. A., Hughes, M., & Harms, C. M. (2005). Testing the effects of nonverbal behavior training on accuracy in deception detection with the inclusion of a bogus training control group. *Western Journal of Communication*, *69*(3), 203–217.

Levine, T. R., & McCornack, S. A. (1991). The dark side of trust: Conceptualizing and measuring types of communicative suspicion. *Communication Quarterly*, *39*(4), 325–340.

Levine, T. R., & McCornack, S. A. (1992). Linking love and lies: A formal test of the McCornack and Parks model of deception detection. *Journal of Social and Personal Relationships*, *9*, 143–154.

Levine, T. R., & McCornack, S. A. (2014). Theorizing about deception. *Journal of Language and Social Psychology*, *33*(4), 431–440.

Levine, T. R., Serota, K. B., Shulman, H., Clare, D. D., Park, H. S., Shaw, A. S., … Lee, J. H. (2011). Sender demeanor: Individual differences in sender believability have a powerful impact on deception detection judgments. *Human Communication Research*, *37*(3), 377–403.

Lewis, J. D. & Weigert, A. (1985). Trust as a social reality. *Social Forces, 63*, 967-985.

Lindlof, T. R., & Taylor, B. C. (2019). *Qualitative communication research methods.* Thousand Oaks, CA: Sage Publications.

Long, J. (2008). *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. (S. Pinzon, Ed.). Burlington, MA: Syngress Publishing, Inc.

Ludwig, S., van Laer, T., de Ruyter, K., & Friedman, M. (2016). Untangling a web of lies: exploring automated detection of deception in Computer-Mediated Communication. *Journal of Management Information Systems*, *33*(2), 511–541.

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

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime, 13*(2), 71-94.

Lyng, S. (1990). Edgework : A social psychological analysis of voluntary risk taking. *American Journal of Sociology*, *95*(4), 851–886.

Mann, I. (2008). *Hacking the human: Social engineering techniques and security countermeasures.* Burlington, VT: Gower Publishing Company.

Mansfield-Devine, S. (2016). The imitation game: how business email compromise scams are robbing organisations. *Computer Fraud and Security*, (11), 5–10.

Manske, K. (2000). An introduction to social engineering. *Information Systems Security*, *9*(5), 53–59.

Massie, S. (2013). *Trust but verify: Reagan, Russia, and me*. Maine Authors Publishing, pp 1-380.

Maurer, D.W. (1940/1999). *The Big Con*. New York, NY: Anchor Books.

Mayer, R. C., Davis, J. H., & Schoorman, D. F. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151–156.

McCornack, S. A., Morrison, K., Paik, J. E., Wisner, A. M., & Zhu, X. (2014). Information Manipulation Theory 2: A propositional theory of deceptive discourse production. *Journal of Language and Social Psychology*, *33*(4), 348–377.

McGuire, M. R. (2018). Cons, constructions and misconceptions of computer. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 1–142.

McHaney, R. George, J.F. & Gupta, M. (2018). An exploration of deception detection: Are groups more effective than individuals? *Communication Research, 45*(8), 1103-1121.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review*, *23*(3), 473–490.

Meissner, C. A., & Kassin, S. M. (2002). “He’s guilty!”: Investigator Bias in judgments of truth and deception. *Law and Human Behavior*, *26*(5), 469–480.

Merton, R.K. (1987). Three fragments from a sociologist’s notebooks: Establishing the phenomenon, specified ignorance, and strategic research materials. *Annual Review of Sociology, 13*, 1-28.

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

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers and Security*, *59*, 186–209.

Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. *Computers and Security*, *55*, 114–127.

National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity* (Version 1.0). Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*, 231–245.

Nyamsuren, E., & Choi, H.-J. (2007). Preventing social engineering in ubiquitous environment. In *Future Generation Communication and Networking (FGCN 2007)* (pp. 573–577).

Pak, J., & Zhou, L. (2014). Social structural behavior of deception in computer-mediated communication. *Decision Support Systems*, *63*, 95–103.

Park, H. S., Levine, T. R., McCornack, S. A., Morrison, K., & Ferrara, M. (2002). How people really detect lies. *Communication Monographs*, *69*(2), 144–157.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Systems Security*, 13–21.

Ponemon Institute, International Business Machines Corporation. (2018). *2018 cost of a data breach study: Global overview*. (Report No. 13). Retrieved from IBM website: https://www.ibm.com/

Porter, S., McCabe, S., Woodworth, M., & Peace, K. A. (2007). "Genius is 1% inspiration and 99% perspiration"... or is it? An investigation of the impact of motivation and feedback on deception detection. *Legal and Criminological Psychology*, *12*(2), 297–309.

Power, R., & Forte, D. (2006). Social engineering: attacks have evolved, but countermeasures have not. *Computer Fraud & Security*, 10, 17–20.

Qin, T., & Burgoon, J. K. (2007). An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering. *Intelligence and Security Informatics, 2007 IEEE*, (July), 152–159.

Rabinovitch, E. (2007). Staying protected from "social engineering." *IEEE Communications Magazine*, *45*, 20–21.

Resnick, P., & Zeckhauser, R. (2002). Trust among strangers in internet transactions: Empirical analysis of eBay' s reputation system. *Advances in Applied Microeconomics*, *11*, 127–157.

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

Rocha Flores, W., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information and Computer Security*, *23*(2), 178–199. https://doi.org/10.1108/ICS-05-2014-0029

Rose, D. R., & Clear, T. R. (1998). Incarceration, social capital, and crime: Implications for social disorganization theory. *Criminology*, *36*(3), 441–480.

Rubin, H.J. & Rubin, I.S. (2005). *Qualitative interviewing: The art of hearing data*. Thousand Oaks, CA: Sage Publications, Inc.

Schaab, P., Beckers, K., & Pape, S. (2017). Social engineering defense mechanisms and counteracting training strategies. *Information and Computer Security, 25*(2), 206–222.

Schlenker, B.R. & Leary, M.R. (1982). Social anxiety and self-presentation. *Psychological Bulletin, 92*(3) 641-669.

Shaw, C., & McKay, H. H. (1969). *Juvenile Delinquency and Urban Areas*. Chicago: University of Chicago Press, p. 140-169.

Sheikhalishahi, M., Saracino, A., Martinelli, F., La Marra, A., Mejri, M., & Tawbi, N.(2020). Digital Waste Disposal: an automated framework for analysis of spam emails. *International Journal of Information Security, 19,* 499-522.

Shover, N., Coffey, G.S. & Hobbs, D. (2003). Crime on the line: Telemarketing and the changing nature of professional crime, *British Journal of Criminology, 43*, 489-505.

Smith, C.A. & Ellsworth, P.C. (1985). Patterns of cognitive appraisal in emotion. *Journal of Personality and Social Psychology, 48*(4), 813-838.

Stewart, S. L. K., Wright, C., & Atherton, C. (2019). Deception detection and truth detection are dependent on different cognitive and emotional traits: An investigation of emotional intelligence, theory of mind, and attention. *Personality and Social Psychology Bulletin*, *45*(5), 794–807.

Steinmetz, K.F., Pimentel, A. & Goe, W.R. (2019). Decrypting social engineering: An analysis of conceptual ambiguity. *Critical Criminology*, https://doi.org/10.1007/s10612-019-09461-9

Sutherland, E.H. (1989). *The professional thief: Annotated and interpreted by Edwin Hardin Sutherland*. Chicago, IL: The University of Chicago Press.

Thompson, H.S. (1967). *Hell's Angels: The strange and terrible saga of the outlaw motorcycle gangs.* New York, NY: Random House.

Tong, S.T. & Walther, J.B. (2010). Just say "no thanks": Romantic rejection in computer-mediated communication. *Journal of Social and Personal Relationships, 28*(4), 488-506.

Tong, S.T. & Walther, J.B. (2015). The confirmation and disconfirmation of expectancies in computer-mediated communication. *Communication Research, 42*(2), 186-212.

Townsend, K. (2010). The art of social engineering. *Infosecurity*, *7*(4), 32–35.

Tsachi, E.D., Perry-Paldi, A., Daniely, T., Zohar-Cohen, K. & Hirschberger, G. (2016). Deciphering the riddle of human deceit detection: groups comprising a higher number of anxious people are better at distinguishing lies from truth. *Psychology, Crime, and Law, 22*(10), 945-956.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: research and practice gaps. *Information Security Journal: A Global Perspective*, *17*, 207–227.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, *52*, 128–141.

Tuttle, H. (2016). The devil in the details: The rise of social engineering fraud. *Risk Management*, 21–27.

Twitchell, D. P. (2009). Social engineering and its countermeasures. In *Handbook of research on social and organizational liabilities in information security* (pp. 228–241).

van den Berg, J. H. (1972). *A different existence*. Pittsburgh, Pennsylvania: Duquesne University Press

van der Walt, E., Eloff, J. H. P., & Grobler, J. (2018). Cyber-security: Identity deception detection on social media platforms. *Computers and Security*, *78*, 76–89.

van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283–297.

Van Swol, L. M., Braun, M. T., & Kolb, M. R. (2015). Deception, detection, demeanor, and truth bias in face-to-face and computer-mediated communication. *Communication Research*, *42*(8), 1116–1142.

Verizon. (2018). *2018 data breach investigations report*. Retrieved May 30, 2019, from https://enterprise.verizon.com/resources/reports/2018/DBIR_2018_Report.pdf

Verizon. (2021). *2021 Data Breach Investigations Report*. Retrieved March 29th, 2022 from https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286–296.

Vernham, Z. Granhag, P.A., & Giolla, E. M. (2016). Detection deception within small groups: A literature review. *Frontiers in Psychology, 7,* 1-13.

von Eckartsberg, R. (1998). Introducing existential-phenomenological psychology. In Valle, R. (ed.), *Phenomenological inquiry in psychology: Existential and transpersonal dimensions* (pp. 3-20). New York: Plenum Press.

Vrij, A., Granhag, P. A., Mann, S., & Leal, S. (2011). Outsmarting the liars: Toward a cognitive lie detection approach. *Current Directions in Psychological Science*, *20*(1), 28–32.

Walther, J.B. (2007). Selective self-presentation in computer-mediated communication: Hyperpersonal dimensions of technology, language and cognition. *Computers in Human Behavior, 23*, 2538-2557.

Weir, G. R. S., Toolan, F., & Smeed, D. (2011). The threats of social networking: Old wine in new bottles? *Information Security Technical Report*, *16*(2), 38–43.

Wertz, F.J., Charmaz, K., McMullen, L.M., Josselson, R., Anderson, R., & McSpadden, E. (2011). *Five ways of doing qualitative analysis: Phenomenological psychology, grounded theory, discourse analysis, narrative research, and intuitive inquiry.* New York, NY: The Guilford Press.

Weiss, R. (1995*). Learning from Strangers: The Art and Method of Qualitative Interview Studies* New York: Free Press.

Williams, J. & Milton T.B. (2015). *The con men: Hustling in New York City*. New York, NY: Columbia University Press.

Whitty, M. T. (2013). The scammers persuasive techniques model. *British Journal of Criminology*, *53*(4), 665–684.

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology and Criminal Justice*, *16*(2), 176–194.

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421.

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273–303.

Wright, G. R. T., Berry, C. J., & Bird, G. (2012). "You can't kid a kidder": association between production and detection of deception in an interactive deception task. *Frontiers in Human Neuroscience*, *6*, 1–7.

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

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662–674.

Worthen, M.G.F. & Baker, S.A. (2016). Pushing up on the glass ceiling of female muscularity: Women's bodybuilding as edgework. *Deviant Behavior, 37*(5), 471–495.

Yasin, A., Fatima, R., Liu, L., Yasin, A., & Wang, J. (2019) Contemplating social engineering studies and attack scenarios: A review study. *Security and Privacy, 2*(4).

Yip, M., Webber, C., Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty, and implications for policing. *Policing and Society, 23*(4), 516-539.

Young, J. (2003). Merton with energy, Katz with structure: The sociology of vindictiveness and the criminology of transgression. *Theoretical Criminology, 7*(3), 389–414.

Zhou, L., & Zhang, D. (2008). Following linguistic footprints: Automatic deception detection in online communication. *Communications of the ACM*, *51*, 119–122.

Zhou, L., Zhang, D. & Y. Sung, (2013). The effects of group factors on deception detection performance. *Small Group Research, 44*(3), 272-297.