2020

Strategies Used to Mitigate Social Engineering Attacks

Lindiwe T. Hove
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Lindiwe Hove

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Bob Duhainy, Committee Chairperson, Information Technology Faculty
Dr. Gary Griffith, Committee Member, Information Technology Faculty
Dr. Jodine Burchell, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Strategies Used to Mitigate Social Engineering Attacks

by

Lindiwe Hove

MS, Walden University, 2016

BS, Minnesota State University, 2013

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

November 2020

Abstract

Cybercriminal activity performed widely through social engineering attacks is estimated to be one of the substantial challenges the world will face over the next 20 years. Cybercriminal activity is important to chief information security officers (CISOs) because these attacks represent the largest transfer of economic wealth in history and pose risks to the incentives for organizational innovation and investment and eventually become more profitable than the global trade of all major illegal drugs combined. Grounded in the balanced control theory, the purpose of this multiple case study was to explore strategies CISOs use to mitigate social engineering attacks within their organizations. Participants consisted of 6 CISOs across 6 small to medium-sized organizations that handle payment card industry data in the West Coast region of the United States of America. Data were collected from CISOs by semi structured telephone interviews. Data were analyzed through interview transcription, in-depth exploration of phenomena, data coding development, and the identification of links to themes. Three major themes emerged from the data analysis: information technology (IT) risks, security awareness, and IT strategies. A key recommendation is for CISOs to develop security awareness programs and implement technical, formal, and informal controls, to sustain operations and protect their networks from potential social engineering attacks. The implications for positive social change include the potential for (a) the mitigation of social engineering attacks, (b) the protection of both organizational and consumer data, and (c) an increase in consumer confidence resulting in increased economic prosperity.

Strategies Used to Mitigate Social Engineering Attacks

by

Lindiwe Hove

MS, Walden University, 2016

BS, Minnesota State University, 2013

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

November 2020

Dedication

This doctoral journey was supported and encouraged by my family, friends, and colleagues. First, this research is dedicated to my parents, who emphasized the importance of higher education and becoming the best that I can be. Second, I dedicate this research study to my husband and siblings. My husband was a constant source of encouragement and understood when I needed to focus on my dissertation and forgo other activities. My siblings provided their encouragement to stay on this path and continue this research study when I encountered challenges. Third, I dedicate this doctoral experience to my living and passed relatives who inspired me to persevere and believe in myself and assured me that I am my ancestors’ wildest dream.

Acknowledgments

I would like to acknowledge my chair, Dr. Duhainy, for providing excellent guidance, answering all my questions, and being responsive throughout this dissertation journey. I would also like to acknowledge my other committee members, Dr. Griffith, for his input, and Dr. Burchell, for providing editorial feedback. Lastly, I would like to acknowledge my numerous colleagues who provided their opinions on information security trends and general thoughts on tackling my doctorate journey. I could not have achieved my research objectives without their participation.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Background of the Problem

Social engineering enables malicious hackers to gain unauthorized access to organizational networks; user accounts and e-mail; databases; smart devices; and electronics, such as laptops, personal webcams, and sensors, including the network connectivity that enables all these objects to exchange data. These hackers use various methods to execute social engineering attacks (Comia, 2017). Cybercrime is on the rise, and social engineering attacks are becoming ever more sophisticated (Cullen & Armitage, 2016a). In this study, I focused on chief information security officers (CISOs) within organizations because they are responsible for ensuring compliance of security procedures and standards as well as making decisions to safeguard security and effect change. There is a need for research on developing a genuinely comprehensive, secure environment (Kim, Kim, Hong, & Oh, 2017).

There is an industry-wide-held belief that when used alone, security tools have proven not to be effective in preventing the detrimental effects of social engineering attacks (i.e., pretexting, phishing/spam, baiting, tailgating, and quid pro quo). The research topic of social engineering, its impact on the security of organizations, and what strategies to implement to mitigate these attacks were formed based on this industry-wide belief. I considered the current mitigation strategies and ongoing challenges to manage it entirely. The outcomes of the study may enable current and future CISOs to understand and implement the plan effectively and safeguard against falling victim to these attacks. The primary research goals of this study were to identify the types of social engineering attacks organizations experience, their severity, current mitigations in place, limitations of those measures, and improvements.

Problem Statement

In 2018, the Department of Homeland Security reported that when successful, social engineering attacks potentially cause businesses to lose their data, reputation, customers, and money. In 2018, the Internet Crime Complaint Center received 20,373 e-mail account compromise complaints (Federal Bureau of Investigation, 2020). The victims reported their business e-mail accounts compromised by social engineering techniques, which prompted them to initiate the unauthorized transfer of funds leading to losses higher than $1.2 billion (Federal Bureau of Investigation, 2018). The general information technology (IT) problem was the failure of organizations to prevent data breaches resulting from social engineering attacks. The specific IT problem was that some CISOs lack strategies to mitigate social engineering attacks within their organizations.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies that some CISOs use to mitigate social engineering attacks within their organizations. The target population consisted of CISOs of six small- to medium-sized organizations that handle payment card industry (PCI) data in the West Coast region and have implemented strategies to mitigate social engineering attacks within their organizations. These strategies may be shared with community leaders to assist with user awareness and reduce the effects of social engineering attacks across their communities. There are several implications of the study for social change. One suggestion from the study, is the prevention of future social engineering attacks, including the theft of confidential data and assets, through the implementation of effective mitigation strategies. The protection of customers' information within the organization's network may increase consumer confidence and result in increased economic prosperity for the local community. Increased economic prosperity would be in the form of economic growth by employing community residents, which would open new public spaces for awareness building and information exchange, thereby fueling the socioeconomic lifecycle.

Nature of the Study

There are three primary methodologies used in scholarly research: quantitative, qualitative, and mixed-method. The methodologies used in qualitative research focus on the exploration and creation of detailed understandings of concepts through one-on-one interviews, facilitated focus groups, or observation (Kaczynski, Salmona, & Smith, 2013). A qualitative method enabled the gathering of in-depth information on how CISOs select strategies and successfully implement them in typically multipronged approaches from detection, training, and simulating the cost of failure to detect. Quantitative research provides the structure and processes to collect, analyze, and evaluate statistical data via tables, charts, graphs, or figures to find associations within a population (Barczak, 2015). A quantitative methodology was not appropriate to explore the strategies used to mitigate social engineering attacks because the method cannot be used to explore to create understanding; instead, it is focused on finding associations within a population. In a mixed methodology, data sets and statistical results from a quantitative method are used along with the data from a qualitative approach to further interpret the reason for a phenomenon (McKim, 2015). A mixed-method approach, due to its inclusion of quantitative methodology, did not serve the goals of this study. A qualitative method was most suited for this study because it enabled the asking of broad questions and collection of data through written and spoken language to explore participants' viewpoints leading to future solutions for social engineering defense.

The qualitative research designs I considered for this study were a case study, phenomenology, ethnography, and a narrative study. A case study design allows detailed, multifaceted exploration of issues of interest through the incorporation of different goals, collection, and data analysis (Ridder, 2017). A case study design was an appropriate design for this study because it could be used to explore specific organizations' successful strategies in mitigating social engineering attacks while offering details from multiple sources through the method of triangulation. By using a phenomenological study design, a researcher seeks to understand subjective experiences from participants who have experienced the phenomenon (Gill, 2014). Unlike a case study design, a phenomenological study was not appropriate for this research because I did not need to explore the lived experiences of employees to address the research question. Ethnographic research focuses on the characteristics of a culture through observation to understand the challenges and motivations and to discover the themes that emerge (Cunliffe & Karunanayake, 2013). An ethnographic study, unlike a case study design, was not appropriate for this research because I did not need to explore the cultural characteristics of the employee or organization to understand their challenges and motivations to discover emerging themes. Because ethnographic research is not used to seek to explore and understand the reasoning behind strategies and their implications, this design was inappropriate for this research study. A narrative study focuses on gathering life experiences through storytelling on how humans experience the world to develop a generalization of what the data means (Kourti, 2016). Unlike a case study design, a narrative study was not appropriate for this research because I did not need to explore the participants' life experiences through storytelling to generalize what the data means. For the purposes of this study, the case study was a more accurate design over the other potential qualitative designs because it is focused on discovering future solutions through exploration and consensus rather than constructing theories.

Research Question

What strategies do CISOs use to mitigate social engineering attacks within their organizations?

Conceptual Framework

I used Dhillon's balanced control theory as the conceptual framework of this study to clarify details of employee behavior and organizational management systems associated with the research. The balanced control theory, developed by Dhillon in 1999, focuses on the implementation of balanced technical systems, formal policies, and informal control strategies to mitigate computer crime (Dhillon, Tejay, & Hong, 2007). The balanced control theory aims to implement control strategies that mitigate computer crime and abuse by employees, and these control strategies comprise preventative measures, such as supervision to reduce the opportunity for a crime and the creation of an environment that fosters a strong sense of moral conscience (Dhillon et al., 2007).

The balanced control theory applied to this research study because it focuses on external attacks and unintentional insider threats resulting from an imbalance of the technical, formal, and informal controls in place. The theory supported the idea that an effective strategy to mitigate social engineering attacks would need to be well balanced by incorporating technical, formal, and informal controls equally. The controls listed by Dhillon and Moores (2001) are: technical (i.e., firewalls, encryption, and password protection), formal (i.e., policies, procedures, and standards), and informal (i.e., training and security awareness).

Operational Definitions

The topic of this study was social engineering attacks within cybersecurity, so I often had to employ technical language. The following definitions provide context to what may be unfamiliar terms.

Hacker: A person external to an organization that uses methods to penetrate the organization's computer system to steal and sell information to other hackers through anonymity techniques (Alazab, 2015).

Social engineering: The process of utilizing human behavior to breach security without the victim being aware they have been manipulated (SysAdmin, Audit, Network, and Security (SANS), 2014). It is an attempt to trick someone into providing confidential information to attack a system or network (Cody, Orebaugh, Scarfone, & Souppaya, 2008).

User awareness: Businesses conduct user awareness training on security vulnerabilities to educate employees on the risks and responsibilities of protecting IT assets (Bhardwaj & Goundar, 2019).

Assumptions, Limitations, and Delimitations

Assumptions

Lips-Wiersma and Mills (2014) defined assumptions as elements that are out of the researcher's control and unverified. The researcher considers assumptions as relevant to the study and correct. I made five assumptions in this research study. The first assumption was that the inclusion criteria for the selected sample were appropriate and representative of targeted information security experts. Another assumption was that participants would honestly answer the interview questions. I also assumed that the information security experts participating in the research study had implemented security controls to minimize data security breaches in the past. It was also assumed that when used alone, security tools have proven not to be effective in preventing the detrimental effects of social engineering (i.e., pretexting, phishing, baiting, and tailgating). The final assumption was that patterns and themes emerging from the data analysis would assist in addressing the research question.

Limitations

Madsen (2013) defined a limitation as a weakness, potentially limiting the scope of the research findings. The primary limitation of this study was the small sample size within the target population, which may have placed a limit on the ability to generalize the research findings (see Pilnick & Swift, 2011).

Delimitations

García, Skotnicka, and Zamora (2015) described delimitations as the boundaries that guide the research study. There were three delimitations of this research study. The first delimitation was that participants were selected based on several factors, including their expertise in information security, social engineering practices, and prior experience in designing information security programs. Another delimitation was that selected participants were currently employed in small- to medium-sized organizations that handle PCI data in the West Coast region. The final delimitation was that participants must have had experience implementing strategies that had improved the mitigation of social engineering attacks within their organizations. By confining the study population to the criteria above, I enhanced the relevance of the findings.

Significance of the Study

Contribution to Information Technology Practice

The value of this study to IT practitioners and their organizations may lie in enhancing their ability to assess and mitigate the impact of social engineering attacks on the security of organizations. Because technical hardware and software have become more sophisticated and challenging to breach, hackers are bypassing these controls and focusing on deceiving individuals to gain access to an organization’s resources (Parmar, 2013). Seventy-five percent of security incidents involve fraud or failure to follow procedure, with unauthorized access accounting for a small percentage of breaches (Wikina, 2014). This statistic on the occurrence of security incidents supports the idea that when used alone, security tools are not as useful in preventing the detrimental effects of social engineering (i.e., pretexting, phishing, baiting, and tailgating) on employees. The findings of this study related to mitigating social engineering attacks may lead to effective IT practice by reducing intellectual property theft and limiting unauthorized access to sensitive data, thereby safeguarding organizational resources. The results of this study may also encourage awareness building and facilitate information exchange within the IT community.

Implications for Social Change

This study contributes to positive social change by providing additional information to leaders in IT on how to protect consumer data through ensuring appropriate defenses are implemented to define and successfully prevent data access through social engineering. Research forms a critical foundation for programs that seek to engage communities in sustainable change; without ongoing research, developed programs are more likely to be based on inferred needs within the community or assumed problem identification. The findings of this study may help leadership identify perceptions within the organizations on the implementation of education, training, procedures, processes, and policy. The findings also provide researchers with validated data that can be used for further studies in this field.

A Review of the Professional and Academic Literature

An organization’s data are one of the most valuable resources they own. Information security is the safeguarding of technology systems and the data they process from internal and external attacks, vulnerabilities, and threats, defined as the triplet asset (Amundrud, Aven, & Flage, 2017). These attacks, vulnerabilities, or threats, whether intentional or unintentional, compromise the confidentiality, integrity, and availability of information (Savola, 2014). Social engineering attacks enable hackers to gain unauthorized access to organizational networks; user accounts and e-mail; databases; smart devices; and electronics, such as laptops, personal webcams, and sensors, including the network connectivity that enables all these objects to exchange data. According to the Institute of Electrical and Electronics Engineers (IEEE) (2018), in the past decade, Internet threats by hackers have transitioned from disabling or destroying government infrastructure to targeting organizations and employees.

From a broad perspective, numerous studies have addressed cybersecurity and insider security threats. Cybersecurity includes cybercrime, such as fraud, data breaches, intellectual property theft, and social engineering. The literature concerning the impact of social engineering in organizations, current mitigation strategies, and ongoing challenges to adequately manage them is insufficient and mostly unresearched. Most of the literature reviewed for cybersecurity focused on technical controls, including software such as firewalls and hardware, which are designed to mitigate hacker attacks using mathematical algorithms. Within the cybersecurity community, how to detect distributed attacks using technical controls has become an essential topic of discussion as are behavior-based approaches that are nontechnical and use learned behavior to recognize future detection (Feng, Hori, & Sakurai, 2017). Sivagnanam (2018) further noted that recent trends, cyberattacks, and technical advancements globally predicted a high likelihood of an organization encountering a data breach within the next 24 months. The gaps in research highlighted the need for the development of effective mitigation strategies to defend against both the technology and human behavior that leads to the success of social engineering attacks.

In this review of professional and academic literature, I provide a critical analysis of the body of knowledge related to the research question. The research is divided into two major categories: social engineering and IT strategies. The social engineering category is subdivided into (a) social engineering attack methods, (b) security awareness, and (c) information security standards. The IT strategies category is subdivided into (a) risk management, (b) employee behavior leading to insider threats, and (c) technology controls.

Information security executives within an organization should be knowledgeable regarding security risks that extend past technology (Njenga & Jordaan, 2016). Security data breaches occur due to weakness in technical and nontechnical controls; nontechnical factors in information security defense include the human/behavioral factor, organizational factors, and environmental factors, all of which are the responsibility of executive management (Henshel, Cains, Hoffman, & Kelley, 2015). According to Farrell (2016), organizations that place equal importance in securing technical and nontechnical controls to protect their information systems are typically more successful in their efforts to mitigate social engineering attacks. Within organizations, CISOs are responsible for safeguarding the security and ensuring compliance of security procedures and standards. The strategies CISOs implement to mitigate these social engineering attacks need to continually evolve to keep up with sophisticated hacker attacks and the latest technology hackers have at their disposal. Focus areas of insider threats within IT include strategy and leadership, security awareness, deception, cyberpsychology, and compliance. From a narrower perspective, a significant lack of research exists on social engineering (Bullée, Montoya, & Pieters, 2015). Within this literature review, I illustrate the evolution of cybersecurity defense, beginning with technical controls, such as hardware and software, and progressing to the inclusion of nontechnical controls, such as organizational and environmental factors. A review of cybersecurity breach reports from organizations in which their implementation of technical and nontechnical controls failed is detailed. I also present current research and theories regarding the human psychology involved in social engineering attacks and characteristics that enabled success as well as identified potential gaps in research.

In the search for literature, I focused on cybersecurity defenses against cybercrime, specifically those leading to social engineering attacks. Both technical and nontechnical controls that play a significant role in cybersecurity defense against social engineering attacks were reviewed. My search for existing research and resources for the current study occurred over 12 months and used a variety of databases. Title searches for literature content were focused on scholarly, peer-reviewed articles, dissertations, books, publications, and conference papers. As a result, the search unveiled several hundred sources for consideration. The published research included perspectives on cybercrime, social engineering attack methods, security awareness, information security standards, risk management, management leadership strategies, employee behavior leading to insider threats, and technology controls. Absent from the literature was a practical standardized approach to implementing solutions for mitigating social engineering attacks.

I found articles, journals, and other resources in the EBSCOhost and ProQuest databases accessed through the Walden University Library, ACM Digital Library, and Google Scholar. Recent publications of the FBI, National Institute of Standards and Technology (NIST), and International Information Security Organization were discovered. Foundational e-textbooks were sourced from industry publications as were white papers from resource organizations, such as the SANS. I focused my search on research published from 2014 to 2019, except for historical sources and supportive theories and frameworks. I conducted a critical analysis and review of the references for this study. The references included 225 articles with 210 (85%) being peer-reviewed journal articles published within the last 5 years (i.e., 2014 and newer) and five seminal books, five government publications, and five non-peer-reviewed articles.

Application to the Applied IT Problem

The purpose of this qualitative multiple case study was to explore the strategies that some CISOs used to mitigate social engineering attacks within their organizations. Cyber attackers implement malicious code to infiltrate and modify organizational data, thereby causing disruptions that can compromise data and lead to cybercrimes, such as data and identity theft (Burnap, French, Turner, & Jones, 2018). Organizations experience one or more of the forms of cybercrime, including worms, Trojan horses, phishing, botnets, and other activities used by cybercriminals to sabotage and attack the organization's systems (Vande Putte, & Verhelst, 2014). The primary information security strategy mostly lacking within organizations is an information security management strategy that encapsulates the technical, formal, and informal systems (Sindhuja & Kunnathur, 2015). Taking into consideration current media reports of security attacks and breaches, the effectiveness of a prevention strategy solely based on technical controls appears to be diminishing. This diminishing effectiveness of technical controls calls for the implementation of new approaches to secure the organizations' systems.

Information security attacks have proven challenging to combat. Barriers include (a) user error or negligence, which occurs by employees violating technical, formal, and informal controls without malicious intent (Dhillon & Moores, 2001); (b) intentionally disruptive actions from both employees and external hackers (Ionescu, Ceaușu, & Ilie, 2018); and (c) non-human-related influences, such as natural disasters. Consideration of fundamental theories that consider the effectiveness of information security based on human vulnerability factors, such as persuasion, cognitive response, and trust, is relevant. An exploration of the occurrence of social engineering attacks due to human vulnerabilities assists with clarification of the issues associated with previous research. Starting in 1985, theoretical explanations of the effectiveness of information system security began to emerge. In the next subsection, I discuss the theory of balanced control by Dhillon et al. (2007), founded on the balance of controls to secure organizational assets and data.

Balanced control theory. The balanced control theory, developed in 1999 by Dhillon, focuses on the implementation of balanced technical systems, formal policies, and informal control strategies to mitigate computer crime. Dhillon et al. (2007) argued that rather than focus on specific information security strategies, a balanced information security approach consisting of technical, formal, and informal controls would be more successful. Dhillon's theory is loosely related to the criminological aspect of the containment theory. The containment theory, developed by Reckless in 1973, suggested that crime prevention is successful when controls are weakened to where they are insufficient in containing motivated behavior in the presence of an unethical opportunity (Kennedy, 2015). Outer containment involves preventative measures and supervision of employees, thereby reducing the opportunity for crime, while inner containment involves the focus on a strong sense of conscience and a positive self-concept (Reckless, 1981).

Dhillon's balanced control theory plays a vital role in information security research. The dependence on information by organizations continues to grow as security breaches continue to escalate, leading to organizations formulating a strategy to secure their information (Horne, Maynard, & Ahmad, 2017). Park, Matkin, and Marlowe (2017) described controls as procedures and rules within organizations used to safeguard assets and detect abuse, waste, and fraud. In this study, I integrated the balanced control theory and focused on external threats and unintentional insider threats resulting from an imbalance of the technical, formal, and informal controls in place.

The balanced control theory supported the idea that an effective strategy to mitigate social engineering attacks would need to be well balanced. This balance is achieved by incorporating technical, formal, and informal controls equally (Dhillon et al., 2007). The controls focused on in this study were technical (i.e., firewalls, encryption, and password protection), formal (i.e., policies, procedures, and standards) and informal (i.e., training and security awareness). I used Dhillon's balanced control theory in this study to clarify details of employee behavior and organizational management systems associated with the research. The balanced control theory is aimed to implement control strategies that mitigate computer crime and abuse by employees (Dhillon et al., 2007). These control strategies comprise preventative measures, such as supervision, to reduce the opportunity for a crime and the creation of an environment that fosters a strong sense of moral conscience (Dhillon et al., 2007).

Dhillon's balanced control theory explains the effectiveness of an organization's IT security as being the result of balanced technical, formal, and informal controls (Dhillon et al., 2007). The balanced control theory aims to implement control strategies that mitigate opportunities for computer crime and abuse by employees through technological and sociological influences (Beebe & Rao, 2005). Atoum, Otoom, and Ali (2017) echoed that implementing cybersecurity is challenging. Organizations successful in mitigating social engineering attacks tend to follow the order of technical, formal, and informal controls (Cuganesan, Steele, & Hart, 2018). Technical controls are based on software and hardware and include firewalls, enforcement of password protection, and encryption to prevent successful attacks (Nishigaki, 2018). Formal controls are comprised of organizational policies, procedures, and standards to introduce checks and balances through outlining acceptable conduct, responsibilities, and supervision. Informal controls are measures that serve to educate employees on the culture of ethics, behavior related to conducting, self-accountability, and self-awareness (Thaler & Helmig, 2016). An effective information security program comprises of controls that cover humans, technology, and processes and are enforced through training programs and a widespread prioritization of ethical behavior and accountability within the organization (da Veiga & Martins, 2015). Informal controls make it clear to employees what behavior reflects the values of the organization and how they will be held accountable for inappropriate behavior and attitudes (Georgiou & Lambrinoudakis, 2017).

If a threat is known, processes implemented by management can deploy preventative measures to control and prevent further damage. For new or unexpected threats, these processes need to be able to promptly respond to control and repair any damages caused by the threat (Baskerville, Spagnoletti, & Kim, 2014). Soomro, Shah, and Ahmed (2016) stated that the management role in information security management should be prioritized to protect the organization.

Organizations should consider incorporating analytical interview techniques and screening processes to aid the employment of honest recruits; these screening processes include conducting criminal background checks, verifying educational skills, and using information interview questions (Padayachee, 2016). Once employed, processes can be implemented to monitor employees' cyber activity (Conteh & Schmick, 2016). Monitoring of employees' cyber activity can be done by implementing time stamp monitoring, security checks, monitoring the use of flash drives and computers, and being attentive to malware and other system breach warnings.

Organizations are reliant on employees, to run efficiently and successfully. As a result, organizations are likely to experience insider fraud by employees (Moghimi &

Varjani, 2016). Management should ensure employees participate in a non-risk policy that works to mitigate carelessness, negligence, and the possibility of employee fraud (Padayachee, 2016). This non-risk policy may include security awareness videos, internal communication campaigns, reinforced seminars, policy violations, and warning messages (Brewer, 2016). The policy works to define parameters and thereby improve the security of the environment.

Organizations are encouraged to provide cybersecurity training programs that cover social engineering to teach employees to recognize the inappropriate cyber activity. These programs should educate employees on major cyber activities, such as the various methods of social engineering and malware intrusions (Brewer, 2016). Cybersecurity awareness programs and skills training are essential to the organization's protection from social engineering attacks (Adams & Makramalla, 2015). Management should encourage employees to report unusual behavior such as unwarranted e-mails or suspicious activities such as unknown individuals requesting access to physical property or the organization's assets.

There has been a steady increase in smartphones and other smart devices within organizations. The advantages of these devices include being able to check e-mail, real-time message chat, access contact lists, and allow employees to run numerous work-related applications. Easy access to a variety of organizational data from smart devices at the touch of a button, has also proven to be a significant concern to the safety of an organization. Markelj and Bernik (2015) noted, when used without the protection of security applications, smart devices can transfer malware and other cybersecurity threats to an organization's network. It was also noted by Tam, Feizollah, Anuar, Salleh, and Cavallaro (2017) that approximately 98% of mobile devices worldwide reported malware infections in 2015. This high infection rate across mobile devices highlighted the importance of organizational policies and employee training in the safe use of smart devices to mitigate cybersecurity attacks.

Organizations are encouraged to seek out partners and third-party suppliers with similar risk appetites and cultures of the organization. An efficient strategy for defusing cyberattacks is the incorporation of protective technologies, across systems that interface each other, that can resolve issues identified for employees, partners, vendors, and suppliers (Manworren, Letwat, & Daily, 2016). To modify security between systems, the assumptions of one subsystem must guarantee the safety of the other (Houser, 2015). This guarantee of security enables an organization to highlight acceptable and unacceptable use policies and provide guidelines for the usage of computer systems, which is essential for the protection of the company's' data and assets. A sub-contracting policy would highlight the need for regular data security audits and the expectation of implemented security measures.

Electronic commerce is crucial for an organization's external business processes as it aids in business-related activities and transactions. Organizations use e-commerce for convenience, transaction efficiency, business cooperation, and virtual production of sales (Wang & Li, 2014). Cybercriminal activity through the manipulation of electronic commerce results in the monetary gain through fraudulent banking transfers, credit card purchases, or the access of an organization's network (Manworren et al., 2016). A breach of an organization supported by electronic commerce does not only affect the business but also affects the customers who may experience identity theft due to their data being accessed, processed, and stored electronically.

Organizations are continuing to innovate their products and service offerings to compete on a global scale. This innovation has led to the use of technology that aids in the quality, speed, and storage of information to provide a means of communication worldwide. Manoj and Bhaskari (2016) noted that the increasingly popular means of storing and protecting financial data and assets is through cloud computing. This technological structure is tailored for business storage. Utilization of cloud computing, while advantageous, creates a new storage facility, which may become an easy target for cybercriminals (Stergiou, Psannis, Kim, & Gupta, 2018). It is essential to place technical security guards to protect this information.

Analysis of supporting security theories

In information system security theories, there are limited theoretical explanations for information security effectiveness that have emerged. There is a need for successful organizations to identify appropriate information security theories for managing an effective IT security program, which includes social engineering mitigation strategies (Kuo, Lin, & Lu, 2017). Knowledge creation has a positive effect on organizational learning (Rezaei, Allameh, & Ansari, 2018). Information security theories guide motivating employees to follow organizational processes successfully. Regardless, organizations tend to learn from both past failures and successes (Matthies & Coners, 2018). Information security theories help executive management understand why employees unintentionally make errors in judgment and provide insight into creating and delivering the right message regarding social engineering mitigation strategies.

Social engineering attacks are founded on biases within the employee's decision making, such as the instinct to trust the hacker. Hackers exploit these biases in various combinations, such as e-mails with exciting content, social media messages, bogus package deliveries, or phone calls to create attack solutions (Jackson, 2018).

There are several trust and information system security theories that guide information security effectiveness. The computational trust theory, general deterrence theory, and cognitive response theory are discussed in support of reasons employees find it challenging to identify social engineering attacks.

Computational trust theory. Computational trust bisects the employee's instinct to trust with the information technology societies, in a less protected environment. With technological advancement, artificial intelligence has transitioned from isolated intelligence to social and collective intelligence (Keating & Nourbakhsh, 2018). Reputation systems increase performance reliability by encouraging honest behavior by providing historical information on the past conduct of users (Wibral, 2015). Computational trust provides a view of information treatments regarding trust and information security. It illustrates how, when implemented together, can counter advanced persistent threats and exploits such as social engineering attacks (Albuquerque, Villalba, Orozco, Júnior, & Kim, 2016). Braga, Niemann, Hellingrath, and Neto (2019) discussed the process of decision making within the computational trust theory. The steps are identification and selection of input data; computing the trust values from the trust evidence; and using the value of trust and risk assessments, resulting in the trust decision being made. Computational trust theory proposing trust and reputation applies to global systems that serve thousands or millions of users (Zhong, Bhargava, Lu, & Angin, 2015). Computational trust theory recognizes trust and reputation systems leveraged by intelligent software agents, as does the behavior trust theory.

Research linking trust to information technology is mostly related to authentication and access control in automation. According to Hoffman and Sollner (2014), research conducted in the behavioral sciences on trust mostly relates to automation and the sociotechnical context of applications. The behavior theory of trust in automation depicts the trust in authenticating access to identify countermeasures. Research has found trust and efficacy can lead to value-added IT use; however, limited research has shown the interplay between both post-adoptive IT use (Tams, Thatcher, & Craig, 2018). Little research has been conducted on developing trust in employee – computer interaction where the human trusts the computer as work is being conducted. The focus of trust research is on the combination of social situations and trust in automation, where employees do not play a role in the process (Wang, Yen, & Tseng, 2015). In behavior sciences, a significant factor studied is users' perception of a system to understand why users trust or distrust a system.

General deterrence theory. The General Deterrence Theory relied on rational decision making and was developed to report the processes and technology involved in the implementation of security measures for computer abuse mitigation (Lee, S., Lee, S. G., & Yoo, 2003). By implementing anti-virus software, enforcing system passwords, and computer security policies, an organization deters external hackers and protects employees from yielding to a hacker's message (Lee et al., 2003). When an employee is exposed to a hacker's message, they are forced to depend on their thought process and rationalization based on the message. While the employee may successfully thwart an external hackers message, an unintentional insider threat, on the other hand, may not be perceived as risky by the employee, which could lead to an attack.

Cognitive response theory. The cognitive response theory supplements human and computer interaction within the effectiveness of IT security. The cognitive response theory was developed to report processes involved in responding to a message. According to Petty, Priester, and Brinol (2009), when responding to a message, individuals depend on their thoughts about the information provided. The theory contends that the impact is dependent on the extent the individual can rationalize their thoughts. An individual response shows participation in the persuasion process (Petty et al., 2009). Individuals reaction to other people or messages is affected by the compelling nature of their initial thoughts.

There are several trust and information system security theories that do not guide information security effectiveness. The systems thinking and action theory and the integrated psychological theory are those discussed that are not supportive in aiding employees to identify social engineering attacks.

Analysis of contrasting theories

In this section, a presentation is made \of both the systems thinking and action theory and the integrated psychological theory concerning Information Security. These theories do not provide sufficient guidance for employees to identify and therefore prevent social engineering attacks.

The systems thinking and action theory. This theory follows the fundamentals and connection of business, society, and economic resources, as well as the control processes within the systems environment. Checkland (2012), noted the four conditions for systems thinking and action to include (a) the acknowledgment of the system and the subsystems, (b) the process of communications within the system, (c) adaptation to change, and (d) defining the emergent properties of the systems environment. For adaptation to be achieved, the system and environment need control processes to initiate change with definable properties, resulting in characteristics of the system about its environment and society. Checkland noted if an action for adaptation persists, the system demands several possibilities of control processes to initiate change. This theory is less useful for reinforcing security within an organization as a critical component of the system within the business is the strategic measures the company implements in its technology to combat vulnerabilities of cybercrime and protection to the organizations' system.

The integrated psychological theory. This theory is an integration of the trait, behavioral, situational, and functional theories while addressing their limitations. The integrated psychological theory introduces the need for leaders to develop an employees’ attitude toward security and behavioral flexibility through the practice of psychological mastery. Employees' behavior is reflective of leadership and, in part, fulfills their daily needs (Lanaj, Johnson, & Lee, 2016). When used alone, theories such as the trait theory are less useful for reinforcing security within an organization as they reinforce the idea that security relies solely on leadership and not employees. Burkus (2015) noted that psychological aspects such as habits or unconscious beliefs could prevent leaders from changing the behavior that freedom of situational, contingency or functional theories offer for differing circumstances.

Analysis of potential themes and phenomena

Potential themes and phenomena for my research study aided in providing a critical analysis of the body of knowledge related to the research question. The themes and phenomena are subdivided into two major categories: social engineering and IT strategies. The social engineering category is subdivided into social engineering attack methods, security awareness, and information security standards. The IT strategies category is subdivided into risk management, employee behavior leading to insider threats, and technical controls.

Social engineering. In this section, I presented themes found predominately in the literature related to social engineering. These themes include (a) social engineering attack methods, (b) security awareness, and (c) information security standards.

Social engineering attack methods. Social engineering attacks use manipulation to target weaknesses. Hackers use deceptive ploys and create compelling behavioral hooks to turn a weak target into disclosing sensitive information (Edwards, Larson, Green, Rashid, & Baron, 2017). There is a notion that human users are the weakest link in information security (Heartfield & Loukas, 2017). As Hadnagy (2014) stated, no information is useless to a hacker formulating a social engineering attack. It is essential to understand the most common social engineering attacks: phishing, pretexting, baiting, tailgating, and quid pro quo.

Phishing is an attempt at gaining unauthorized access to sensitive information. Phishing is the use of fraudulent e-mails or impersonating websites that hackers use to convince employees to share valuable personal or employee confidential information such as social security numbers, login credentials or passwords (Federal Trade Commission, 2018). Phishing e-mails enable hackers to infiltrate an organizations' network by encouraging employees to open malicious attachments and links (Williams, Hinds, & Joinson, 2018). A phishing e-mail may be targeted to an employee, have a credible logo, contain a URL leading to a login page with the request to verify credentials, or be an urgent message soliciting an immediate response. Although becoming more sophisticated, the majority of phishing messages can be analyzed and found to be written in poor grammar, contain a misleading link within the phishing message, or lead to a false domain (Jensen, Dinger, Wright, & Thatcher, 2017).

Pretexting is a technique where a hacker creates a fictional situation to gain sensitive information. Pretexting involves impersonating an authority figure, trusted individual, or fellow employee to gain access to organization login credentials (Wu, Lee, Lin, & Wang, 2014). One example of pretexting is voice disguise; used by hackers to evade identification while sounding genuine (Singh, Jiménez, & Øland, 2017). Impersonation plays a huge role in influencing employees to fall victim to social engineering deception (Algarni, Xu, & Chan, 2017). The individual then becomes trusted and permitted to gain access to personal or organizational confidential data.

Baiting is a technique used by hackers to entice employees to provide sensitive information. Baiting involves the luring of an employee toward taking a specific action the hacker desires (Internal Revenue Service, 2018). Techniques such as baiting through e-mail are preferred by hackers, compared to using technical means to hacking e-mail accounts (Zingerle, 2014). An attacker can seize remote access to an organization's network if they are skillful with baiting an employee to open the connection (Atwell, Blasi, & Hayajneh, 2016). If the employee proceeds to take the requested action, malicious software may autoload and enable the hacker to gain access to the individual's computer system.

Tailgating, also known as piggybacking, involves the hacker who lacks authorization, attempting to gain physical access to a restricted area. Hackers can gain entry into restricted areas simply by tailgating (Sreevidya & Sumanta, 2016), which involves entering the restricted area by following someone who has legitimate access (Aurigemma and Mattson, 2017). A common tailgating example is that of a hacker requesting an employee to hold an entryway door open under the guise of having forgotten their access card. Another guise involves a hacker requesting physical access to an employee's mobile device or computer system with the intent to install malicious software.

Quid pro quo involves a hacker requesting an employee for access to user or organization data in exchange for something. Quid pro quo is a social engineering technique used to entice employees (Lord, 2018). The promise of a gift or desired service is commonly used to tempt an employee to provide access (Dara Security, 2015). Quid pro quo takes advantage of the employees' vulnerability to tempt them to provide unauthorized access.

Security awareness. Security awareness is a process where employees are educated about IT protection. A survey conducted by Pricewaterhouse Coopers (2015) focused on the state of cybercrime within the US. The survey indicated the annual financial losses for organizations that provided security awareness training was $162,000, in comparison to annual financial losses of $683,000 reported by organizations that did not provide security awareness training (Pricewaterhouse Coopers, 2015). The importance of improving personnel training when it comes to security awareness due to global trends in the development of information society is emphasized by Belov, Los, and Malyuk (2018). A study on security compliance and training by the International Information System Security Certification Consortium (2016), was highly regarded, with 42% of respondents being organizational leaders indicating that their employees are currently their greatest vulnerability to cyberattacks. The conducted study also showed that some respondents viewed security awareness training as ineffective on its own. This lack of effectiveness in regards to security awareness training was largely due to organizational leaders acknowledging employees not being cybersecurity experts and, as a result, not expecting them to guard against security threats (International Information System Security Certification Consortium, 2016).

Participants in the state of cybercrime study (Pricewaterhouse Coopers, 2015) argued that a sole focus on security awareness training diverts organizational resources from other more serious challenges such as flaws in software design or technical controls. Small to medium-sized organizations that handle payment card industry (PCI) data are required to create and maintain written security awareness policies and procedures to adhere to industry regulations (SANS, 2014). Compliance with industry regulations requires security awareness documentation to account for both internal and external technological advances and threats. While organizations are investing significant resources in security awareness training, as data breaches continue to grow, the effectiveness of training is questioned (Rashad, 2014).

As part of their daily business transactions, organizations are tasked with safeguarding confidential records of both their clients and vendors. These records are stored to enable organizations to foster customer relationships, target marketing campaigns, and increase sales activities (Bobitan & Stefea, 2015). Arhin and Wiredu (2018) added that information is one of the organization's most important assets. The information needs to be accurate, complete, and available for the organization’s decision-makers to enable processes and business strategy development (Otto, 2015). Organizations need to implement established and regulated industry best practices and standards to protect these critical technology assets (NIST, 2018). In addition to information being valuable, the security of the technology systems that store this information is vital to the continued operation of the organization.

The standard setting encourages conformity and provides a baseline from which to assess and measure the performance of a product or service. Standardization, according to NIST (2018), provides foundational best practice requirements that must be met by organizations. Standards provide world-class specifications for products or services to ensure their quality, efficiency, and safety (International Organization for Standardization (ISO), 2018). Technology standardization provides baseline requirements that are agreed upon within industry; this agreement subsequently forms the foundation of technology interoperability (Jiang, Zhao, Zhang, & Yi, 2018). Security standards related to technology primarily focus on the logical and physical specifications that ensure the security of computer systems. Leadership management standards focus on a series of behaviors and a set of systems that are implemented (Barrow, 2016). The ISO/IEC 27001 standard illustrates a process for implementing and managing information risks by outlining procedures to identify, operate, analyze, clarify, remediate and maintain security management systems and security governance (Alebrahim, Hatebur, Fassbender, Goeke, & Côté, 2015). ISO 27001 furnishes security experts and organization executives with a framework to align their objectives.

Information security standards. Standards like the ISO 27001 provide organizations with a template that they can implement to ensure effective security controls and procedures are in place, thereby safeguarding their key asset, information. ISO 27001 enables organizations to identify the risks, vulnerabilities, and threats to their organizational strategies (ISO, 2018). Performance evaluation within the standard focuses on risk management and enables leaders to create their custom security management framework (Alebrahim et al., 2015). The other information security standards that organizations can use to base their security programs off are Information Security Forum, The Standard of Good Practice for Information Security, Generally Accepted Information

Security Principles, and the NIST Cybersecurity Framework. Information security programs provide framework templates on which organizations can develop and implement their technology security policies, procedures, and strategies.

The Data Security Standard, published by the Payment Card Industry Security Standards Council, seeks to provide a minimum set of required security controls to protect cardholder data. There are still doubts regarding the Payment Card Industry Security Standards Council compliance and its ability to provide an acceptable level of security. Numerous organizations that have followed and implemented security controls and procedures, as per the standards, have experienced the failure of these measures in mitigating security threats (Yang, Lee, Park, & Eom, 2015). The rise in data breaches during PCI compliance has led some organizations into allocating resources away from detective controls and into preventive controls (Moldes, 2018). Organizations that handle PCI data are heavily regulated and obliged to adhere to industry set standards. Effective security management strategies are crucial in the success of security initiatives and mitigation of security breaches (Abrahamsen, Aven, Pettersen, Kaufmann, & Rosqvist, 2017). Security experts and executive management are encouraged to rely on both security procedures and management of their computer systems to ensure both compliance and mitigate data breaches

IT strategies. To further provide a critical analysis of the body of knowledge related to the research question, this section focuses on IT strategies. The strategies were subdivided into risk management, employee behavior leading to insider threats, and technical controls.

Risk management. Risk management is a business strategy employed within organizations to develop business and mitigate events that may cause harm to the organization. Risk management is the process whereby business risks are identified and used to develop a strategy that will detect, minimize, and respond to risks (Lin, Rivera, Abrahamsson, & Tehler, 2017). Implementing various methods to identify business risks is crucial as risks, and risk types are uncertain. Risk management plays a crucial role in identifying situations involving risk where loss is probable. Risk management, while complicated, adds immense value to an organization and aids in promoting competitive advantage (Vilko, Ritala, & Hallikas, 2016). Lekaj and Kercini (2017) emphasized this thought by adding that executives within an organization need to fully understand and appreciate business risks and the vulnerabilities their information assets have.

The focus of management within this growing competitive market is on sustainable business decisions and risk management. Risk management offers an integrated approach for organizations by paving the way for a basis to improve, coordinate and align their organizational risk processes to enable process improvement (Barafort, Mesquida, & Mas, 2018). Information security risk management enables organization executives to align business and system risk into their organizational strategy (Jedynak & Bąk, 2018). The identification of risk can determine and influence organizational management processes (Brožová, Šup, Rydval, Sadok, & Bednar, 2016). Anderson (2017) discussed the need for organization executives to have access to up to date information on emerging risks and risk mitigation strategies. Executive involvement in risk management ensures support and investment in information security initiatives.

The rate of failure for new businesses is high in their first year of operation. According to the Bureau of Labor Statistics (2016), studies show 8 out of 10 businesses fail within their initial 2 years of operation. Launching a new business or product is risky; therefore, how management assesses and reduces risk is a critical factor in the success or failure of a business or product (Snell, 2015). Business risks include processes, people, systems, and events that should all be considered when ensuring adequate risk management (McKim, 2017). Management needs to be aware of business risks that may lead to failure and develop mitigation strategies to avoid a crisis. As noted by Gendron, Brivot, and Guénin-Paracini (2015), management executives and their corporate boards are concerned and more proactive towards organizational exposure to risks.

Information security risk assessment is the core of information security. Information security risk management is an integral part of an organization's business strategy and risk mitigation as it protects information availability, integrity, and privacy (Amine, Mostafa, & Wissam, 2016). Organizational security risks include the unintentional disclosure of organization sensitive and proprietary information by employees. Most of the leakage of organizational data has been reported as occurring through e-mail, instant messaging, and cloud applications (Hatice, Seref, & Yavuz, 2017). Managing the risks associated with unintentional disclosure of organizational information is a crucial concern for executive management which makes proactive detection of ongoing attacks critically important (Awad, Gill, Lee, Kadry, & Maddodi, 2016)

Social engineering attacks take advantage of the human tendency to trust. These attacks where humans tend to trust each other lead to them readily disclosing to hackers, organizational or personal information (Junger, Montoya, & Overink, 2017). As cybersecurity threats continue to grow, they have led to reports of social engineering and the compromise of the organizational e-mail being the two most rising threat vectors (Carlton & Levy, 2017). This form of manipulation convinces the employee to trust that the request is legitimate. Due to their trusting nature, employees within the organization may provide this access or information unintentionally (Li, Liu, & Sonali, 2017)

Social engineering attacks are noted to be difficult to detect and protect against due to their target of both humans and hardware or software systems. Bakhshi (2017), studied two attack scenarios using social engineering techniques. Despite revealing signs of an attack before the test, 46 – 60% of the employees failed to identify the attacks when exposed. Unintentional employee actions have been shown to occur due to negligence or carelessness (Mouton, Leenen, & Venter, 2016). Employees, in this case, also termed unintentional insider threats, have been noted in most data breaches to be the weakest link in an organization's security chain (Greavu-Şerban & Şerban, 2014).

Employee behaviour related to security. Employee behavior related to security is comprised of two elements, the unintentionality of providing information and the knowledge of the human element in social engineering through the hacker. An employees' likelihood of providing information to a hacker unintentionally may be related to their technical expertise and knowledge of organizational security (Mironela, 2017). From this perspective, non-technical knowledge relates to the employees' awareness of organizational security regulations and security-related policies and procedures (Rocha & Ekstedt, 2016). Social engineering has become a severe threat in communities and an effective means to attack information systems within organizations (Krombholz, Hobel, Huber, & Weippl, 2015).

Employees targeted by hackers to conduct their social engineering attacks are perceived to be the weakest link to providing access to enable a breach of the organization's security. Information within an organization is a crucial resource (Ahmad, Bosua, & Scheepers, 2014). For a breach in security to occur, a single point of entry within a chain of connected devices or services needs to be intercepted for a hacker to gain access to the organization's information. Regardless of the strength of perimeter security, within organizations, there are numerous opportunities for malware attacks to penetrate the network undetected (Kedgley, 2015). These types of social engineering attacks are based on both a psychological and a physical perspective. To gain physical access to an information system, rather than forcibly entering an organization's network using computer algorithms, a social engineer uses psychological means to gain the trust of an employee and perform their deceit (Mansfield-Devine, 2017).

The end goal for a hacker performing social engineering attacks is to persuade the employee to divulge confidential information. The use of technology to perform social engineering attacks has aided hackers seeking access to organizational assets and access to intellectual property. Organizational strategies for mitigating these attacks through internal organization settings are lacking (Jayakar, 2018). Existing literature has depicted primary defense strategies of technology controls utilized through hardware and software.

The prevention of social engineering attacks was primarily researched in the information security field in the past decade. Fellnhofer (2018), highlighted that the main research topics in the past decade had been centered around information security assessments, risk management, information security strategic planning, technical aspects within information security, development, and monitoring of information systems. In the past decade, internet threats by hackers have transitioned from disabling or destroying government infrastructure to targeting organizations and employees (IEEE, 2018). Security infrastructure and intrusion prevention and detection systems continue to evolve to mitigate security attacks such as social engineering attacks (Airehrour, Nair, & Madanian, 2018). Honeypot systems and other network services serve as traps for detecting and deflecting hackers from an organization's actual sensitive network system. Fatna, Younes, and Habiba (2017) listed the two benefits of deploying a honeypot approach as the ability to harvest the information of hacker profiles and the ability to analyze the characteristics of these hacker profiles and those of deployed honeypots to create classifiers allowing the constant modification of new profiles. The development of honeypot systems is essential for the future of information systems. The development of software to further refine honeypot-based detection to prevent botnet attacks has been discussed in detail by Rajarajan and Ganesan (2017).

Technology controls. With ongoing technical developments, cryptography has become a widely accepted and industry expected technical control for preventing sensitive information access to attackers. Cryptography is defined by Faisal and Maaruf (2018) as the hardening of network devices, operating system features, management controls, access-list restrictions, operational configurations and ensuring organization data and credentials are not stored or transferred through the network in 'plaintext.' The process of cryptography includes constructing and analyzing protocols that prevent attackers from gaining access by converting information from a legible state to an illegible state (Walaa, Jamal, & Bani, 2017). Cryptography and encryption are terms that are used interchangeably (Edwards, 2014). Encryption within organizations has increasingly become enforced by industry standards and regulations as a means of securing their communication by providing data integrity, confidentiality, and authentication (Achuthshankar, Achuthshankar, Arjun, & Sreenarayanan, 2016). With improvements in technology, encryption methods have become increasingly complex.

As with technical controls, security data breaches also occur due to weakness in non-technical controls. Information security executives within an organization should be knowledgeable regarding security risks that extend past technology (Njenga & Jordaan, 2016). Non-technical factors in information security defense include the human/behavioral factor, organizational factors, and environmental factors, all of which are the responsibility of executive management (Henshel et al., 2015). To ensure the success of implemented security processes and procedures, specific managerial activities are required to encourage a security mindset among employees (King et al., 2018). There is less emphasis on non-technical controls within the information security industry. As a result, the success of non-technical factors in mitigating social engineering attacks has received less attention from the researching community and organizations that are prone to cybersecurity attacks. Nontechnical controls can also be segmented into formal and informal (not enforced by the organization) controls.

Formal controls have evolved to keep abreast of both technological advancements and cybersecurity attacks. Formal controls are comprised of organizational measures for acceptable use and behavior policies, procedures, and standards (Cordell, 2015). The information technology security infrastructure has expanded to include formal organizational controls such as policies for risk management, information security policies, standards, checklists, and the technical controls within security (Younis, Kashif, & Madjid, 2014). Within organizations, formal controls have become inclusive of physical security. The growing number of breaches has highlighted the insufficient attention paid to both technical and human aspects within cybersecurity in organizations (Furnell & Vasileiou, 2017). The mitigation of social engineering attacks has become reliant on an employee's knowledge about their technical expertise and their awareness of the security policies and regulations implemented by the organization. Security within an organization is reliant on both the technical and non-technical controls being secured.

Security trends and mitigation of social engineering attacks requires a holistic approach. This holistic approach covers the various vulnerabilities within an organization's system infrastructure (Woods, Agrafiotis, Nurse, & Creese, 2017). An organization's system infrastructure is typically protected by risk management policies, information security policies, standards, checklists, and technical controls within security. Lack of an implementation of this complex organization system infrastructure leads to a broad attack surface posing security risks and vulnerabilities (Rao, Carreon, Lysecky, & Rozenblit, 2018). According to Farrell (2016), organizations that place equal importance in securing technical and non-technical controls to protect their information systems, are typically more successful in their efforts to mitigate social engineering attacks.

Organizational aspects within information security are known to at the forefront of mitigation strategy discussions within the technology field. These factors fall under organizational culture and organizational security awareness (Scholl, Leiner, & Fuhrmann, 2017). To ensure the success of information security programs within an organization, it is essential to optimize the integration of the security culture and security awareness. Researcher Laskowski (2017) has shown that an organizations' vision and goals should be well aligned with implemented security controls to mitigate the risk of data loss. This balance works to promote the delivery of value within the organization. As with non-technical controls, information security research has mostly paid less attention to the inclusion of both security culture and awareness in building a successful information system that mitigates social engineering attacks (Woo, Cerveny, & Sanders, 2018)

Informal controls within an organization are framed around the employee's conduct. These range from self-control, accountability, attitude awareness, and ethical issues. Thaler and Helmig (2016) discussed the increasing importance of management of ethics as well as codes of conduct and ethical leadership, which has led to a positive effect on employee's organization related attitudes. A positive effect on employees shows an increase in productivity, effectiveness, and efficiency (Veronika, Klára, Krisztina, László, & Edit, 2016). Five main controls have been determined to be effective in protecting an organization's data from security breaches. These are: the incorporation of the model of cybersecurity governance as determined by the National Institute of Standards and Technology framework; establishing policies regulating the use of information assets; establishing a code of conduct for its employees; developing a corporate security culture and; maintaining a corporate security department (Terlizzi, Meirelles, & Viegas, 2017)

Relationship of this study to previous research.

Prior research has been conducted on the analysis of various individual information security strategies and the approaches used to discover, detect, and prevent security attacks. Previous research has intended to provide evaluations of data collected and evaluate the best strategy (Chang, Kuo, & Ramachandran, 2016). With the increasing advanced security attacks, further research is crucial in malware detection and prevention for social engineering mitigation in organizations. This study combines the consideration of various individual information security strategies, processes, and career experiences of CISOs, to provide additional research in the successes of an implementation balanced information security approach.

Organizations should consider incorporating analytical interview techniques and screening processes to aid the employment of honest recruits. These screening processes include criminal background checks, verifying educational skills, and using information interview questions (Padayachee, 2016). Once employed, processes can be implemented to monitor employee’s cyber activity (Conteh & Schmick, 2016). Monitoring can be done by implementing time stamp monitoring, security checks, monitoring the use of flash drives and computers, and being attentive to malware and other system breach warnings.

Organizations are reliant on employees to run efficiently and successfully. As a result, organizations are likely to experience insider fraud by employees (Moghimi & Varjani, 2016). Management should ensure employees participate in a non-risk policy that works to mitigate carelessness, negligence, and the possibility of employee fraud (Padayachee, 2016). This non-risk policy may include security awareness videos, internal communication campaigns, reinforced seminars, policy violations, and warning messages (Brewer, 2016). The policy works to define parameters and thereby improve the security of the environment.

Organizations are encouraged to provide cybersecurity training programs that cover social engineering to teach employees to recognize inappropriate cyber activity. These programs should educate employees on major cyber activities such as the various methods of social engineering and malware intrusions (Brewer, 2016). Cybersecurity awareness programs and skills training are essential to the organization’s protection from social engineering attacks (Adams & Makramalla, 2015). Management should encourage employees to report unusual behavior such as unwarranted e-mails or suspicious activities such as unknown individuals requesting access to physical property or the organization's assets.

There has been a steady increase in smartphones and other smart devices within organizations. The advantages of these devices include being able to check e-mail, real-time message chat, access contact lists, and allow employees to run numerous work-related applications. Easy access to a variety of organizational data from smart devices at the touch of a button, has also proven to be a significant concern to the safety of an organization. When used without the protection of security applications, smart devices can transfer malware and other cybersecurity threats to an organization's network (Markelj & Bernik, 2015). It was also noted by Tam et al., (2017) that approximately 98% of mobile devices worldwide reported malware infections in 2015. This high rate of malware infections across devices worldwide highlights the importance of organizational policies and employee training in the safe use of smart devices to mitigate cybersecurity attacks.

Organizations are encouraged to seek out partners and third-party suppliers with similar risk appetites and cultures of the organization. An efficient strategy for defusing cyberattacks is the incorporation of protective technologies, across systems that interface each other, that can resolve issues identified for employees, partners, vendors, and suppliers (Manworren et al., 2016). To modify security between systems, the assumptions of one subsystem must guarantee the safety of the other (Houser, 2015). This assumption of security enables an organization to highlight acceptable and unacceptable and provide guidelines for the usage of computer systems, which is essential for the protection of the company’s data and assets. A sub-contracting policy would highlight the need for regular data security audits and the expectation of implemented security measures.

Electronic commerce is crucial for organizations' external business processes as it aids in business-related activities and transactions. Organizations use e-commerce for convenience, transaction efficiency, business cooperation, and virtual production of sales

(Wang & Li, 2014). Cybercriminal activity through the manipulation of electronic commerce results in the monetary gain through fraudulent banking transfers, credit card purchases, or the access of an organization's network (Manworren et al., 2016). A breach of an organization supported by electronic commerce does not only affect the business but also affects the customers who may experience identity theft due to their data accessed, processed, and stored electronically.

Organizations are continuing to innovate their products and service offerings to compete on a global scale. This innovation has led to the use of technology that aids in the quality, speed, and storage of information to provide a means of communication worldwide. Manoj and Bhaskari (2016) noted the increasingly popular means of storing and protecting financial data and assets is through cloud computing. This technological structure is tailored for business storage. Utilization of cloud computing, while advantageous, creates a new storage facility that may become an easy target for cybercriminals (Stergiou et al., 2018). It is essential to place security guards to protect this information.

Transition and Summary

In summary, information security attacks pose an ever-increasing risk to individuals, organizations, society, and global entities by infiltrating computer networks and gaining unlawful access to confidential data (Hu, Xu, M., Xu, S., & Zhao, 2017). Cybercrime is on the rise, and social engineering attacks are becoming ever more sophisticated (Cullen & Armitage, 2016a). The financial, legal, and reputational costs to organizations following a cyberattack are far-reaching. Organizations have a responsibility to all stakeholders to safeguard their information and ensure it's not accessible to hackers; unfortunately, reports of organizational data breaches remain a commonplace. CISOs need to become knowledgeable regarding the risks of cyberattacks directed at their organizations and work toward mitigating these attacks. An exploration of attack mitigation strategies may aid organizations in preventing cyberattacks

Section 1 was a description of the security threats to system infrastructure and data within organizations. Within this section, an emphasis was placed on the importance of technology leaders to understand and actively practice IT strategies and policies that work to address data security problems. I discussed the background of the problem, the problem and purpose statements, the nature of the study, research question, conceptual framework, operational definitions, assumptions, limitations, delimitations, the significance of the study, and a review of the literature. Within the literature review, I outlined social engineering attack methods, security awareness, information security standards, risk management, technical and non-technical controls. Section 2 is an overview of the research project, which includes the purpose statement, my role as a researcher, participants, the research method.

Section 2: The Project

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies that some CISOs use to mitigate social engineering attacks within their organizations. The target population consisted of the CISOs of six small- to medium-sized organizations that handle PCI data in the West Coast region that had implemented strategies to mitigate social engineering attacks within their organizations. These strategies may be shared with community leaders to assist with user awareness and mitigate the effects of social engineering attacks across the general population. The findings of this study positively contribute to social change by paving the way for IT leaders to open new public spaces for awareness building, discussion of critical issues, and the facilitation of information exchange.

Role of the Researcher

Serving as the primary collection source within the data collection process was my role as the researcher. A researcher faces a host of decisions regarding the approach to take, the type of interviews to conduct, and the method to be used to collect information (Yates & Leggett, 2016). As a cybersecurity specialist, I possessed knowledge in the areas of social engineering attacks and their repercussions on an organization. I did not have a prior relationship with the research participants. According to Calverley, Foulds, Nordhagen, O’Keefe, and Xinfang (2014), researcher expertise in a subject area plays a crucial role in establishing and maintaining credibility.

As a researcher, I also had a role to play regarding ethics and following *The Belmont Report* protocol. I reviewed *The Belmont Report*, which is a guideline for ethical principles and the protection of human subjects in research, and the report calls for researchers to respect participants, to maximize the benefits of the study design while trying to minimize any risks, and to select research participants impartially (see U.S. Department of Health & Human Services, 1979). I completed the Protecting Human Research Participants training offered by the National Institutes of Health (NIH) Office of Extramural Research (Certification Number: 2281166; see Appendix A). NIH participant protection training, as noted by Resnik, Miller, Kwok, Engel, and Sandler (2015), assists researchers in the informed consent process, the protection of participants, and dealing with ethical challenges in research. Onwuegbuzie and Hwang (2014) suggested bias mitigation in that researchers should refrain from asking leading questions. I mitigated bias by avoiding both making assumptions and asking leading questions when conducting interviews with participants.

I developed an interview protocol to help conduct the interviews in a manner that allowed the participants to convey insights on social engineering and mitigation strategies implemented within their organization. A case study protocol provides reliable data collection guidance to a researcher (Yin, 2013). As detailed by Bölte (2014), the use of interviews in data collection enables the researcher to gain a deeper understanding, from the participants' perspectives, of the research topic. Foley and O'Conner (2013) emphasized that using an interview protocol ensures consistency and reliability over the course of the qualitative research process. I used the interview protocol with each participant.

Participants

Researchers need to state the guiding principles and criteria used to select participants, so other researchers can assess the transferability of the criteria-based research findings (Elo et al., 2014). As highlighted by Nadal et al. (2015), following the participant selection criteria firmly is also essential to protecting participants. A relationship that encourages transparency, trustworthiness, and respect is essential between the researcher and participants (Bowden & Galindo-Gonzalez, 2015).

The participants in this study were six CISOs from small- to medium-sized organizations with experience in mitigating information security attacks within organizations. As leaders of their respective organizations, the participants were responsible for ensuring compliance with security procedures and standards and making decisions to safeguard security and effect change (see Wara & Singh, 2015). Participant requirements also included current, full-time employment within the IT departments in the PCI, a minimum of 10 years of information security industry experience, and residency in the West Coast region. The organizations in this multiple case study had not reported any social engineering attacks within the past 3 years, per the inclusion criteria.

To gain access to the participants, I attended conferences and peer interaction opportunities held by Infragard. InfraGard is a partnership between the FBI and members of the private sector for the protection of U.S. critical infrastructure (Infragard, 2019). This organization is comprised of over 50,000 business executives, entrepreneurs, lawyers, security personnel, military, and government officials, IT professionals, academia, and state and local law enforcement that understand the criticality of information security and pledge to improve business. Infragard serves as an industry leader in information security education, collaboration, and information sharing. To identify the potential participants, I used the searchable member repository, which is accessible by keyword, specific industry, job title, chapter location, country, and state. I cross-referenced the search results with The Breach Level Index (BLI). BLI (2018) is a worldwide database that tracks publicly disclosed breaches and provides researchers with valuable information for security research and validation. According to Wara and Singh (2015), a sophisticated cyberattack can trigger a crisis that can affect both internal and external stakeholders. An awareness of the existence of sophisticated cyberattacks leads to the need to examine breach data repositories on which the cyberattack analyses would be based.

To establish a working relationship with potential participants, I drafted an introductory letter that was sent via my Walden University e-mail account. In the introductory letter, I described the study, the role participants would play, and potential time commitments as well as my contact information. Upon receipt of the participant's acknowledgment of my letter and willingness to participate, a working relationship was formed. Avoidance of microaggressions, which are subtle forms of discrimination, and working toward building a relationship based on mutual respect and trust were essential skills to master (Nadal et al., 2015). To this end, I fostered an environment for open communication in which participants could trustingly engage in the research process.

Arguing in favor of interviews to gather information, Bowden and Galindo-Gonzalez (2015) expressed that research participants, when faced with the researcher, can see each other and use social cues, such as body language to avoid ambiguity and misinterpretation of messages exchanged. Rossetto (2014) found that research interviews can be therapeutic for both the participants and the researcher, which is crucial to the success of the case study.

Research Method and Design

Method

Three primary methodologies are used in scholarly research: qualitative, quantitative, and mixed method. A researcher’s beliefs and experiences may play a role in the questions they ask survey respondents as well as how those responses are interpreted (Leppink, 2017).

A qualitative methodology paves the way for research questions to be open to unexpected findings (Tavakol & Sandars, 2014a) with the choice of design depending on the nature of the research problem and scientific knowledge being sought (Korstjens & Moser, 2017). A qualitative methodology is exploratory and used to understand human behavior, conceptual phenomena, groups, or individuals as opposed to numerical data in quantitative research (Yin, 2013). In comparison to a quantitative method in which the researcher is isolated from the phenomenon, the qualitative method allows a researcher to obtain user data from a participant to address the research question. Qualitative research encompasses a broad range of philosophies, approaches, and methods, which, when used, enable a researcher to acquire an in-depth understanding of people’s perceptions (Vass, Rigby, & Payne, 2017). Methodologies within qualitative research focus on the reasoning of a participant to obtain results that are (a) focused on a worthy topic, (b) include productive rigor, (c) sincere, (d) credible, (e) resonate, (f) provide a significant contribution, (g) ethical, and (h) provide meaningful coherence. A qualitative method was the best choice for this study because qualitative descriptions were essential to exploring the mitigation strategies CISOs implement to protect their organizations from cyberattacks.

A quantitative methodology is used to examine variables and the testing of hypotheses (Boyle, Whittaker, Eyal, & McCarthy, 2017) with probability and statistics determined within a population (Barnham, 2015). The measurement tools used in quantitative research aid in the validity and reliability of a study (Tavakol & Sandars, 2014a). Quantitative research provides the structure and processes to collect, analyze, and evaluate statistical data via tables, charts, graphs, or figures to find associations within a population (Barczak, 2015). The context of this study was in mitigation strategies for social engineering attacks without the intention of testing hypotheses, seeking statistical data, or generalizing the data across other non-IT attacks on organizations. The quantitative method was not appropriate for this study because it requires a hypothesis test.

A mixed methodology is used to examine data sets and statistical results from a quantitative method along with the data from qualitative methods to further interpret the reason for a phenomenon (McKim, 2015). A researcher uses mixed methods to examine relationships and differences between variables utilizing a central research question and hypothesis (Venkatesh, Brown, & Bala, 2013). Mixed methods provide researchers with the option to combine participants' experiences with empirical data to determine the relationship between specific variables (Yin, 2013). A mixed-method study combines the best of qualitative and quantitative methods (Leppink, 2017). A mixed-method component relies on a combination of experiences, hypotheses, and relationships among variables, which was not my intention in this study. A mixed methodology was not appropriate for this study because the participants' experiences did not be combined with empirical data to address the research question.

Research Design

I considered a case study, phenomenological, ethnography, and narrative research designs for this study. Each of the four qualitative research designs has its strengths and weaknesses (Almalki, 2016). Yin (2013) noted that a rigorous research design is essential and expertly guides a researcher throughout the study.

I selected a multiple case study design for this study. The nature of this design is gathering detailed and multifaceted opinions (Ridder, 2017). Multifaceted opinions allowed for the exploration of social engineering mitigation strategies through the incorporation of different goals, collections, and data analysis. Carolan, Forbat, and Smith (2016) described that the use of multiple data sources typifies this research approach. Data sources can include observation, interviewing, recording, or documenting participant information (Yin, 2013). The data collection methods within the design provide a holistic approach focused on variables in a natural setting and working toward understanding participants' perceptions and interpretations (Cope, 2015). With the case study design, a researcher illustrates the viewpoints of participants through incorporating numerous data sources to determine how participants gain knowledge and make decisions regarding an event (Yin, 2013). A case study was appropriate for this study because it focused on discovering future solutions through exploration and consensus. The case study design supported the purpose of this research study, which was to gather the opinions of CISOs and seek a consensus on strategies and solutions for mitigating social engineering attacks.

Researchers incorporate a phenomenological design study to understand participants versus a phenomenon (Gill, 2014). According to Roberts (2013), this design best explores participants' lived experiences. Using the participants' experiences, the researcher gains an insightful understanding of the phenomenon (Koçyigit, 2017). A phenomenological study was not appropriate for this research because I was not exploring participants' lived experiences with the phenomenon.

Ethnographic researchers focus on the characteristics of a culture, through observation, to understand the challenges and motivations of the culture and to discover emergent themes (Cunliffe & Karunanayake, 2013). According to Cruz and Higginbottom (2013), this understanding of cultural groups occurs through observations conducted over prolonged periods. Ethnography is a means to represent a group graphically and in writing within the context of their culture (Knobloch et al., 2017). Because I was not exploring the cultural characteristics of a group to understand their challenges and motivations or to discover emerging themes, an ethnographic design was not appropriate for this study.

A narrative researcher focuses on gathering participants' life experiences for storytelling on how humans experience the world and to develop a generalization of what the data means (Kourti, 2016). Tamboukou (2011) stated that a narrative design should be used when exploring a biographical study that follows the lives of individuals. Lewis (2015) explained the role of researchers in a narrative study as the exploration of how participants view themselves and their experiences. Because I did not focus on gathering participants' life experiences for storytelling on how humans experience the world, a narrative study was not appropriate for this study.

Population and Sampling

The population for this study was CISOs across six small- to medium-sized organizations within the PCI industry from the West Coast region of the United States. To understand the population, the definition of small to medium-sized businesses is 499 or fewer employees (Alkhoraif, Rashid, & McLaughlin, 2018). The West Coast region is among the highest concentration of technology companies handling PCI of all regions in the United States. A justification of the population serves to demonstrate saturation within the dataset (Gentles, Charles, Ploeg, & McKibbon, 2015). The population and sample size are measured by the depth of data rather than frequencies, which enables the selection of participants to consist of the best to answer the research topic (Cho & Lee, 2014). Participants were recruited by obtaining the CISOs name, e-mail address, location, and a number of employees from IT membership databases such as Infragard, which is a partnership between the FBI and members of the private sector for the protection of U.S. critical infrastructure. The prospective participants received an invitation via email to participate in the research study via a telephone interview. Attached to the email was an informed consent form, which provided detail about their inclusion in the study. All participants must have successfully implemented strategies to deter cybercrime and mitigate social engineering attacks and were willing to provide this information within the interview.

Purposive sampling for this qualitative case study was appropriate for this research study. Purposive sampling enabled me to deliberately select participants based on specific individual characteristics that pertain to the subject matter being researched (Barratt, Ferris, & Lenton, 2015). Purposive sampling is a nonprobability sampling technique whereby the researcher is encouraged to use their best judgment to select participants that will provide unique and rich information of value to the study (Suen, Huang, & Lee, 2014).

Ames, Glenton, and Lewin (2019) described purposive sampling as ensuring the sampled population represent a wide geographic spread, assist in gathering rich data and aid in a focus closely resembling the study objective. Due to the wide population purposive sampling represents, it was suitable for case study research. I selected a purposive sample of CISOs from the population of small- to medium-sized organizations that handled PCI data within the West Coast region of the United States from IT membership databases. This selection of potential participants provided information to enable me to conduct purposeful sampling in the recruiting of eligible participants.

Within qualitative research, the sample size is selected to be adequate to identify the themes within the research study. A researcher chooses the number of participants, which depends on the topic and availability of resources (Benoit, Hannes, & Bilsen, 2016), and uses this sample to gather a rich data set. Within qualitative research, there is a point of data saturation reached whereby continuing to collect data only serves to confirm emerging themes (Fusch & Ness, 2015). The goal of a researcher obtaining an appropriate sample is to ensure a detailed analysis of the phenomenon through the selection of individuals is presented (Kwong et al., 2014). In a case study, the sample size can consist of 4 – 15 participants to reach saturation (Gentles et al., 2015). I interviewed CISOs in six small- to medium-sized organizations with twelve-open ended questions, which provided enough data to achieve data saturation. If saturation had not been reached, I would have interviewed additional CISOs.

CISOs within organizations are responsible for ensuring compliance with security procedures and standards and making decisions to safeguard security and effect change (Wara & Singh, 2015). In addition to implementing design and enforcing security policies, they recommend security investments (Karanja, 2017). I selected CISOs within small- to medium-sized organizations that handle PCI as these types of organizations face significant data security threats due to their increased adoption of online, mobile, and smart device banking applications (Martins, Oliveira, & Popovič, 2014). My selection of local organizations was to enable easier identification of local participants.

Data saturation has an impact on the quality of research conducted. According to Fusch and Ness (2015), data saturation is reached when enough information has been gathered to replicate the study, no additional new information is available, and further coding is no longer feasible. A researcher’s failure to reach data saturation diminishes the validity of one’s research (Walker, 2012). Kwong et al. (2014) noted that qualitative researchers should continue interviewing participants until data saturation is reached. I conducted interviews with CISOs in six small- to medium-sized organizations that handle PCI data in the West Coast region. I selected some participants until no new themes emerge, and I reached data saturation.

The interview process catered to the interviewees' availability to allow accurate data collection through open-ended questions, with the possibility of follow up questions that could provide additional clarity and validation for the study (Houghton, Murphy, Shaw, & Casey, 2015). It was my obligation as the researcher to interview in a natural setting (Nadal et al., 2015). This natural setting assisted with performing data analysis that is both inductive and deductive toward establishing patterns and themes (Elo et al., 2014). An interview also provides clues in cases of loss of nonverbal data and contextual data (Goodman-Delahunty, Martschuk, & Dhami, 2014). It is essential to promote a comfortable, natural setting to gain the participant's confidence and support while creating an asymmetric power relationship between the interviewer and the interviewee (Robinson, 2014). Also, Robinson (2014) emphasized the importance of allowing the interviewee to contribute to the study. The contribution sought from interviewees details their experiences, expectations, and predicaments on an interview topic through a conversation rather than an interrogation.

Ethical Research

When designing and researching a qualitative multi-case study, ethical standards need to be adhered to during several phases of research, including ethical issues of sensitive information of participants (Yin, 2017). Before the collection of data from selected participants, approval from the Institutional Review Board (IRB) ensures ethical standards and requirements are implemented. Also, a researcher requires specific conditions to allow access to their data (Nadal et al., 2015). Following approval from the IRB to initiate the research study, I e-mailed the identified prospective participants and invited them to participate in the study. Interviews provided participants with the information regarding the purpose of the interview, the research subject, the data collection process, and the informed consent form. The rights of participants are protected, and the ethical value of participant autonomy is upheld (Chiumento, Khan, Rahman, & Frith, 2015). I followed the research ethics and standards provided by the National Institute of Health and completed training on protecting human research participants. The training emphasized confidentiality as a critical element of qualitative design, thereby ensuring no identification of participants or their organizations. The research participants provided written consent. This informed consent form included additional detail regarding the participant's rights and acceptance for participating in the study. The participant had the option to withdraw from the study without penalty through contacting me via e-mail or telephone. Participants did not receive monetary payments or any other incentives to partake in the study. To ensure their anonymity, participants received an identification code of P-1, P-2, P-3, and so on. As outlined *in the Belmont Report,* as a researcher, I adhered to three core ethical principles (a) Respect for persons, (b) beneficence, and; (c) justice for every participant (U.S. Department of Health & Human Services, 1979). I will secure all forms, field notes, transcripts, and data to be collected in a locked box within a locked cabinet in my home for 5 years, following the conclusion of the research study. At the end of the 5-year data retention period, I will shred and destroy the data.

Data Collection

Instruments

As a researcher, I was the primary data collection instrument. The concept of the researcher within qualitative studies being the primary data collection instrument is echoed by Råheim et al., 2016). Anleu, Blix, Mack, and Wettergren (2016) discussed the role of being the primary data collection instrument, where the researcher is responsible for collecting data in a natural setting to assist with performing data analysis that is both inductive and deductive to establish patterns and themes. The cultural notions of authority and position within the research relationship need to be taken into account (Probst, 2016). Qualitative data collection is comprised of building trust with participants.

When conducting data collection, qualitative researchers use semi-structured interviews (Janghorban, Roudsari, & Taghipour, 2014). Semi-structured interviews have been noted as a valid data collection instrument (Pezalla, Pettigrew, & Miller-Day, 2012). I used open-ended questions (Appendix B) within the data collection instrument. The interview questions were open-ended to stimulate more interaction within the participants. Open-ended questions pave the way for case study researchers to gather insights on specific issues under study (Yin, 2013). Through the use of semi-structured interviews, researchers can uncover hidden facets of human and organizational behavior due to the participant's openness to respond in the best way they know how to interview questions. Semi-structured interviews enable participants to provide an in-depth understanding of a research topic (Yin, 2013). A semi-structured interview is an appropriate approach to capture detailed information about the participants' expectations, views, and experiences (Izci, & Göktas, 2017). The use of semi-structured interviews has been discussed by Thompson (2017) as enabling the researcher to gain insights into participant's perspectives about their practices.

Using an interview protocol will assist in increasing the reliability of a case study research (Yin, 2013). Member checking and thematic analysis aid in adding validity to the study (Comley-White & Potterton, 2018). I avoided bias by avoiding leading questions. Posing the same interview questions in a sequence to research participants helps to identify themes and allows for efficient data analysis and response comparison (Brédart, Marrel, Abetz-Webb, Lasch, & Acquadro, 2014; Hermanowicz, 2013). Researchers, however, should refrain from asking leading questions in interviews in a manner that leads to bias (Onwuegbuzie & Hwang, 2014). In addition to asking the same questions and avoiding bias, I used multiple data sources for methodological triangulation. Methodological triangulation increases the credibility, reliability, and validity of the study (Yin, 2013). Multiple data sources that were used for this study included utilizing publicly available security and privacy policies implemented in organizations. It was noted by Saunders and Townsend (2016) that the process of efficient participant interviews includes reporting, justification, and several interview participants selected within an organization. Archived data, such as documentation and recordings from interviews, provided qualitative research data.

Methodological triangulation provides the researcher with an in-depth understanding of the phenomenon in the study. The use of multiple data collection methods is necessary for the alignment of data and essential for considering trends in data (Komisar, Novak, & Haycock, 2017). Wierenga, Engbers, van Empelen, Hildebrandt, and van Mechelen (2012) added that methodological triangulation enables researchers to probe for patterns within the data to develop overall interpretations using multiple perspectives. An increase in confidence within the study findings is evidenced through the researcher's use of multiple sources in the mitigation of research biases (Harrison, Banks, Pollack, O'Boyle, & Short, 2014).

Member checking was also implemented within the interview process to aid in research validity and the reduction of bias. Member checking assures rigor with research case studies, as discussed by Houghton, Casey, Shaw, & Murphy (2013). Member checking included providing participants via email, a summarized interpretation of their interview responses. The summarized interpretation enabled them to view my interpretation of their responses. Member checking provided a researcher with an opportunity to ensure data saturation had been reached. Also, it enables a researcher to seek participant’s verification of the accuracy of the interview response (Culver, Gilbert, & Sparkes, 2012). Member checking is also utilized for quality control to verify and validate data collected during the research interviews (Harper & Cole, 2012).

Data Collection Technique

Data collection began following IRB approval. The participants that had met the research criteria and received the invitation to participate in the study contacted me via e-mail. When a participant agreed to participate in the research study, the participant received the consent form and reviewed it. The consent form detailed the research study topic, sample research questions, the voluntary participation and withdrawal process, disclosure of incentives, and how the data would be safeguarded. Once I received the participant's consent, I scheduled a convenient date and time for them to participate in a telephone interview. All the research participants received before the interview, a copy of the interview questions to review (Appendix B).

The primary data collection technique was the interview, which lasted approximately 30 minutes. The open-ended questions listed in Appendix B encouraged the conversation and captured the necessary data to address the research question. Open-ended questions pave the way for case study researchers to gather insights on specific issues under study (Yin, 2013). Utilizing semi-structured interviews enables data collection to take place through a flexible, intelligible, and accessible approach (Qu & Dumay, 2011). The interviewer encourages interviewees to recall and report all relevant information they can remember (Vrij, Mann, Jundi, Hillman, & Hope, 2014). All interviews were recorded using my laptop digital recorder, and a smartphone recorder available as a backup. These interview recordings assisted with the data analysis process for the research study (Al-Yateem, 2012). Voice recordings made following consent by the participants were analyzed by content analysis to identify themes (Güngör, & Özkara, 2017). Researchers can use recorded interviews to learn and understand participants' experiences and gain self-awareness and insight into the role they played during the research and how it benefitted them (Barkham, & Ersser, 2017). Following the interview, the audio was transcribed using the voice to text application, Voice Recorder. I concurrently reviewed the transcribed text while listening to the audio to ensure accuracy and form my interpretation of participants' responses for member checking.

I utilized the process of member checking to assure response validity. Member checking assures rigor with research case studies (Houghton et al., 2013). A researcher performs member checking to consider the accuracy of the participants' interview responses (Harvey, 2015). Each interview response was summarized for thematic analysis and member checking to illustrate emerging themes from individual responses. Member checking is a technique for exploring the credibility of results and will provide the research with a means to test and fit their interpretation to participants' responses (Smith & McGannon, 2018). Data or results were returned to participants to check for accuracy and resonance with their experiences. Participants were requested to comment on the narrative summary to ensure their views were well understood. In the data analysis process, feedback received from participants was incorporated, and themes that emerged in the study were confirmed.

Each data collection technique has its advantages and disadvantages. Document reviews are timeous to collect, review, and analyze the data (Owen, 2014). The advantage of document reviews is their inexpensiveness, provision of in-depth, rich background information, and their ability to highlight issues not yet discovered by other data collection methods (Wolfswinkel, Furtmueller, & Wilderom, 2013). Elo et al. (2014) highlighted the primary disadvantage of conducting interviews, is the risk of interview bias. However, interviews encourage participants to elaborate and discuss in-depth issues that are important to them (Pacho, 2015). Within this study, I conducted interviews with the study participants and collected, archived data through the form of publicly available documentation.

Data Organization Techniques

The data collection for this qualitative multicase study was of responses by CISO's of small to medium organizations gathered through telephone interviews with open-ended questions. Data organization techniques are used by researchers when managing data to ensure the reliability and validity of a study (Martin & Meyer, 2012). Each participant recording was stored on a new USB flash drive, labeled with their identification code such as P-1, P-2, P-3, and so on. According to Jamshed (2014), a researcher can focus on the content of the interview and transcribe it easier when it is recorded. The USB flash drive that connects to the laptop digital recorder allowed the transfer of the recordings for transcription. Following the transcription of interviews using the Voice Recorder, voice to text application, I organized the transcripts within a Microsoft Word document. Once the original interview has been transcribed, and member checking has occurred, the researcher establishes data credibility (Harvey, 2015). Member checking provides a researcher with an opportunity to seek participant's verification of the accuracy of the interview response (Culver et al., 2012). A research log captures data to aid in the examination of assumptions and actions thematic within the study (Wagstaff, Hanton, & Fletcher, 2013). This research log provides an audit trail that the researcher can rely on to identify and reflect on challenges occurring during the study and minimize potential bias throughout the study (Georgiou, Marks, Braithwaite, &

Westbrook, 2013). The member checked transcripts, research logs, and archival documents were uploaded into QSR NVivo. QSR NVivo is a computer-assisted qualitative data analysis software (Bergin, 2011), used for data collection, management, and analysis of qualitative audio and written data (Castleberry, 2014). This uploaded information was organized into categories for thematic analysis in QSR NVivo. This qualitative research will organize data into categories that will assist in identifying themes during data analysis (Merriam, 2014). Yin (2013) adds that the identification of emerging patterns, themes, and trends from interviews is the focus of data organization. I will store the interview recordings, transcripts, and research logs on an encrypted hard drive solely accessible by me for five years.

Data Analysis Technique

The objective of the data analysis process was for an evaluation of patterns and themes that emerged during the interview process. Data analysis involves the application of principles such as interview transcription, in-depth analysis of phenomena explored, data coding development, and the identification of links to themes (Smith & Firth, 2011). Yin (2017) added that emerging patterns are identified through analytical techniques, which result in the strengthening of the validity of the study. The use of multiple sources of evidence in case study research allows the researcher to explore various evidence and converging lines of inquiry (Yin, 2017). One such analytical technique is triangulation. Through triangulation, a researcher can explore multiple sources of information to strengthen the construct validity of the study (Morgan, 2019). Methodological triangulation involved using more than one method to gather data, such as interviews, observations, questionnaires, and documents. I used methodological triangulation to analyze data obtained from open-ended interviews and peer-reviewed studies detailing cybercrime prevention strategies.

Choosing the most significant research study participants to obtain detailed data was more significant in comparison to sample size when reaching data saturation. Data analysis relied on data saturation is reached. Fusch and Ness (2015) detailed data saturation to include (a) no new data obtained, (b) no new themes identified, (c) no new coding, (d) the ability to replicate the study. I selected participants that have successfully implemented social engineering mitigation strategies to prevent breaches and protect their organization from cybercrime attacks. I continued to interview participants until data saturation was reached. To ensure the credibility and validity of the information gathered through the interviews, member checking was conducted for each interview. The data analysis process continued with an in-depth evaluation of themes and patterns that emerged from the interviews. I uploaded, organized, and analyzed the transcribed interview data within the QSR NVivo qualitative software to organize the data, identify meaningful units, and develop emergent themes for triangulation.

I applied a data coding process to categorize data by source types such as acquired documents and interview data to identify emerging themes. Coding qualitative data involves identifying common categories within the data, ideas, and themes to enable analysis, organization, and comparison of data to extract meaningful information (Zamawe, 2015). Within QSR NVivo, coding data leads to the creation of nodes (Ferrer & Ruiz, 2017). Each node was a collection of references to a specific theme, place, or person. When coding, I created nodes with the interview transcripts and accumulated documentation. Nodes represented the data source types and the following categories for data analysis (a) cybersecurity breaches, (b) incident response strategies, (c) risk management, (d) Information security policies/standards, (e) organizational performance, (f) data security governance. The categories for data analysis represented successful organizational components.

Reliability and Validity

Reliability and validity eliminate bias and minimize errors within qualitative research. According to Elo et al. (2014), there are four criteria to help ensure reliability and validity. These criteria are dependability, credibility, transferability, and confirmability. Reliability and validity are both crucial in qualitative research studies as they help ensure the data is trustworthy. I used open-ended questions that promoted in-depth responses from CISOs regarding managerial strategies implemented successfully to combat cybercrime.

Reliability

The goal of establishing reliability is to eliminate bias in the research study and minimize any errors (Cope, 2014; Noble & Smith, 2015). Reliability is the consistency of results obtained. Reliability is a criterion for judging the quality of research study designs, with the logical test of the research findings being data dependability (Yin, 2013). To establish reliability, researchers in qualitative studies use dependability to focus on a measurement formed within a construct (Cope, 2014). The following section highlights the establishment of dependability of the study findings.

Dependability

Dependability, according to McCusker and Gunaydin (2015), refers to research data remaining the same under different conditions. The researcher establishes dependability and trustworthiness through reporting the content analysis obtained from the data collection method, sampling strategy, and data analysis techniques selected (Hays, Wood, Dahl, & Kirk-Jenkins, 2016). Thomas (2017) explained that the dependability of the data presented is reliant on the interaction between the researcher, the research study, research data, and a high level of accuracy. Dependability was achieved within this study through recording and reviewing transcripts, member checking, and additional note-taking during the interview process.

Validity

Researchers aim to establish the validity of the research tool to ensure that the selected instrument most relates to the construct of interest and will assist in answering the research question. Validity aims to minimize errors, eliminate bias, establish integrity, and applicability of the methods in use, all while ensuring precision in which the findings accurately reflect the data (Noble & Smith, 2015). According to Yin (2013), researchers ensure validity by focusing on the measurements between constructs. Trustworthiness, credibility, and conformability are logical tests guiding qualitative research. Three criteria assist in judging the quality of research designs: construct validity, internal validity, and external validity (Yin, 2013). Within a qualitative research study, these criteria for establishing validity are in the form of creditability, transferability, and confirmability

(Cope, 2014). The following sections discuss how creditability, transferability, and confirmability of the research findings was established.

Creditability

In qualitative research, rather than the term validity, creditability is used. According to Cope (2014), creditability refers to the truth of the data and the views of the participants. As researchers are the research instruments, the creditability of the study is ensured through the dependence on procedures implemented, and the researchers self-awareness throughout the research process. Noble and Smith (2015) listed methodological strategies used to ensure creditability in findings as a reflection on the researcher's perceptions, using a representative sample on the phenomenon; achieving audit ability and application of conclusions to other contexts.

To ensure credibility for the study, I used methodological triangulation and member checking. The purpose of methodological triangulation was to increase confidence in research data by utilizing and confirming multiple data sources to reduce bias (Hays et al., 2016). I triangulated interview data, with peer-reviewed studies, to address the research question. Harvey (2015) described member checking in qualitative research as participant validation that aids in improving the accuracy, credibility, and dependability of data received within the interview. I performed member checking by emailing a copy of the analysis to participants following the initial interview and verifying the accuracy of the information through a follow-up telephone interview. In addition to methodological triangulation and member checking for credibility, I adhered to the research method, design, data collection through participants responding to identical interview questions and data analysis described. White, Oelke, and Friesen (2012) detailed data saturation as a critical element in ensuring credibility in qualitative research. I achieved data saturation using purposive sampling, which was supported by the identification of participants with rich experiences within cybersecurity. I continued interviewing participants until no new themes emerged.

Transferability

Qualitative researchers provide detailed descriptions of the research process, which the readers use to determine the transferability of the study. According to Cope (2014), transferability refers to the application of findings to other settings or similar groups. Purposive sampling is used to enhance the transferability of findings (Maree, Parker, Kaplan, & Oosthuizen, 2016). The research structure, which includes purposeful sampling and details, an outline of research assumptions, limitations, and delimitations, provided sufficient context for determining the transferability of this study by other researchers. Transferability is the ability to generalize research findings to a larger population (Marshall & Rossman, 2010). Transferability is essential as it allows researchers in the future to build on the study or develop a new theory (Elo et al., 2014). Transferability will be achieved if the findings of a qualitative study are transferable to similar settings (Hays et al., 2016).

Confirmability

Confirmability is based on the confirmation of findings and logic of the data following its analysis (Pozzebon, Rodriguez, & Petrini, 2014). Confirmability ensures the researcher represents a participant’s response rather than the researcher's bias (Cope, 2014). Member checking of each interview will ensure the validity of the research process and achieve confirmability (Hays et al., 2016). The recognition of limitations of the study and audit trail enhances confirmability (Maree et al., 2016). The development of an audit trail, which included note taking during the interview and member checking, helped to foster confirmability that was used within this study.

Transition and Summary

The focus of this qualitative case study was to explore the strategies implemented by CISOs to mitigate social engineering attacks. In Section 2, I restated the purpose of the study and highlighted the role of the researcher, the participants, the research method, and design. Also, I discussed population sampling, ethical guidelines, data collection instruments, techniques, organization, analysis, and concluded with the reliability and validity of the study.

Section 2 contained a justification for the decision to use a qualitative multiple case study design. The most appropriate research method and design was the qualitative multiple case study, as it explored mitigation strategies CISOs implement in the protection of their organization's data and mitigate future attacks on their systems. Before data collection, I completed an oral defense and obtained permission from the IRB to begin my research.

In Section 3, I present detailed research study findings and their application to professional practice. I highlight the implications for social change, recommendations for action, and future research and conclude with a reflection of my experiences performing the study.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore the strategies that some CISOs use to mitigate social engineering attacks within their organizations. The data came from six research participants across six organizations who were (a) CISOs, (b) had experience in small- to medium-sized organizations that handle PCI data, (c) were in the West Coast region, and (d) had successfully mitigated social engineering attacks. The conceptual framework for this study was the balanced control theory. Participant interview responses provided the data used to address the research question. The three major themes that emerged were (a) IT risks, (b) security awareness, and (c) IT strategies. The research findings showed methods that the CISOs successfully used to mitigate social engineering attacks to safeguard the security of their organizations.

Presentation of the Findings

The research question for the study was: What strategies do CISOs use to mitigate social engineering attacks within their organizations? I used archived, publicly available documentation and participant interviews conducted with open-ended questions (see Appendix B) to collect data for this study. Data saturation was achieved when interview respondents’ data presented no new information or themes. As the primary research data collection instrument, I created a folder of participant correspondence, interview summaries, and related peer-reviewed studies. The research analysis was conducted by importing the data into QSR International NVivo.

My analysis of interview data and publicly available institutional reports enabled triangulation in the data collection process. To maintain participants' confidentiality, the following participant codes were used: Participant 1 (P1), Participant 2 (P2), Participant 3 (P3), Participant 4 (P4), Participant 5 (P5), and Participant 6 (P6).

All participants defined social engineering as manipulative techniques used by cybercriminals to gain access to a system and confidential information. P1 described social engineering as a "technique to manipulate the users." P2 explained that "the primary motivation of social engineering is to gain access to a company's system and network or lure people to providing sensitive information such as bank account and credit card information for financial gain." P3 added that social engineering is a "technique to trick people," while P4 similarly declared that it is a "tactic…to exploit people." P5 added that "hackers lure people into breaking security procedures to gain access to networks and systems for financial gain." P6 expanded on previous explanations by stating that the techniques could either exploit weaknesses in people or on a company's infrastructure. P6 further explained that social engineering is a "tactic used by hackers to exploit people by using loopholes in a company's policy or a person's emotions." Some of the techniques discussed by the participants included phishing and malware attacks.

Based on the frequency of coded node responses, three major themes emerged from the triangulated data analysis: (a) IT risks, (b) security awareness, and (c) IT strategies. In the following subsections, I detail the three identified themes. Each theme presented showcases the considerations made by CISOs to successfully mitigate social engineering attacks. Figure 1 provides a visual of the relationship of the IT risks, security awareness, and IT strategies that would result in an overall risk management strategy to reduce social engineering risks.

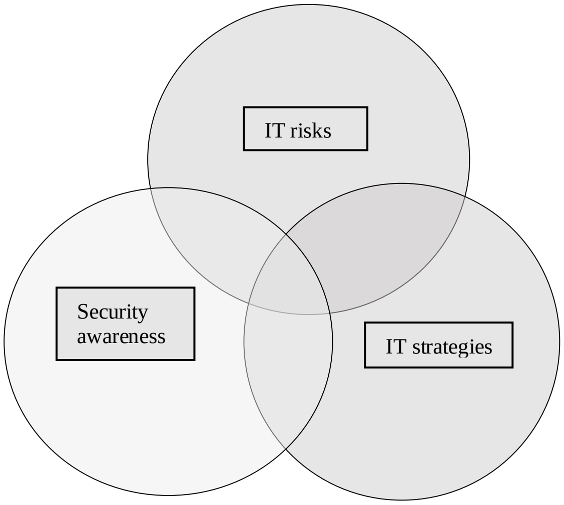


Figure 1. Relationship of themes showcasing overall risk management strategy.

Theme 1: IT Risks

The first significant theme identified during the NVivo data analysis was the importance of identifying technology risks and the use of various policies and procedures to prevent, limit, or respond to social engineering attacks. Most respondents said they do not have or advise a one-size-fits-all technology risk assessment model (see Table 1). The respondents added that when developing a model, it is essential to consider factors such as the value of assets, size of an organization, resources, and growth rate. However, they felt that there were essential elements that the models needed to have to make them useful. Common among all respondents was the identification of threat sources. They kept abreast of trends in security threats by networking with organizations within the same industry. A significant security concern was the current COVID-19 pandemic where attackers may trick users into providing sensitive information under the guise of cures and relief packages. In this regard, P1 reported that "the current pandemic has led to an increase in social engineering attacks with people e-mailing or calling about fake cures or the stimulus package passed by Congress."

Table 1

Information Technology Risks

	Participant count	Document count
No one size fits all	4	4
Identification of threat source	6	4

The next element for assessing IT security risks was impact analysis. Respondents first identified the critical assets and sensitive data within the organization, developed a risk profile, and then determined the extent of loss in case the assets were compromised. In explaining the process, P4 reported that the first step is to "identify the most vulnerable data in your network. Secondly, you need to have a risk score of the associated loss of data (the more the effect, the more careful you have to be)". P4 concluded that the third element was implementing mitigation and preventative measures. One of the measures to mitigate the likelihood of threat, identified by P4 was installing software updates, "then follow the mitigation model like upgrading for windows seven to windows ten and such."

Respondents deemed prevention as one of the most important measures. These included limiting unauthorized access to sensitive information by redacting information from documents, encrypting data, and granting data access rights to a limited number of people. In citing an example of limiting unauthorized access, P3 explained that "role-based access is assigned to roles that can access confidential information, such as an expert witness, a sting operation, and a production environment." Technical controls, such as setting up firewalls, were also listed. The respondents also implemented user training aimed at making users aware of possible threat actions. In this regard, P4 added that "prevention is always better than fixing the hack, such as implementing mitigating factors for phishing e-mails and random phone calls from strangers requesting information like a password, through user security awareness training." Mock tests helped them in assessing user awareness levels. To this end, P2 stated the importance of "assessing the level of social engineering awareness within the team. This level of awareness includes phishing attempts to see their response and Pen tests to see if the IT team is aware." P2 further explained that the last and final element was documenting the results of assessment exercises, stating, "Have a risk assessment report on all departments."

Publicly available literature concerning ongoing challenges to fully manage social engineering attacks is insufficient and mostly unresearched. There are several challenges that respondents discussed facing regarding the mitigation of social engineering attacks. One of the main challenges faced by respondents when responding to social engineering attacks is noncompliance from employees. The respondents felt that threat events posed the greatest challenge to the fight against social engineering threats. They reported cases where employees leaked information despite having prior knowledge of control measures. Besides, it was easy for insider attackers to develop circumventing tools because they were already privy to existing security control measures. To this end, P5 noted that “sometimes, the social engineering threat could be a student or an employee; hence, if they are aware of the measures taken to prevent social engineering, they could come up with new tactics.” To improve compliance, respondents felt it was essential to create organization-wide training on potential risks. P6 highlighted,

> how one responds to that is you have to provide the people in the organization; whether they’re in the IT shop or elsewhere in the organization and they touch technology in any way, they need to be prepared on what the risks are, what they look like.

Social engineering threats are hard to detect. Respondents felt that cybercriminals are good at their jobs and know whom and where to hit. Employees are, mainly, an easy target. Participant P4 believes “those behind social engineering attacks are brilliant and intellectual individuals who can manipulate the user’s mind and get access to digital personal data. Therefore, the first challenge is even noticing the hack itself.”

The third challenge was the ever-changing threat landscape. Security control measures that were effective today could be ineffective tomorrow because cybercriminals are always trying to come up with more sophisticated attacks. Hence, respondents said that it was essential to have frequent and ongoing training to keep users abreast of current risks. In this regard, P6 stated,

> people in the organization need to be prepared on what the risks are, what they look like, and as we mentioned already that keeps changing. It’s nothing that you can do once a year; you have to keep doing it year-round.

Finally, respondents felt that the social engineering risk management process was resource intensive. In particular, it required a lot of time to train users as well as funds to purchase training materials. P1 explained that “It is time consuming to train and educate people on social engineering since some people get knowledge faster than others. Also, the materials required for education on social engineering are costly.

The balanced control theory aims to implement control strategies that mitigate computer crime and abuse by employees. These control strategies comprise preventative measures, such as supervision to reduce the opportunity for a crime and the creation of an environment that fosters a strong sense of moral conscience (Dhillon et al., 2007). Organizations successful in mitigating social engineering attacks tend to follow the order of technical, formal, and informal controls (Cuganesan et al., 2018). Technical controls are based on software and hardware and include firewalls, enforcement of password protection, and encryption to prevent successful attacks (Nishigaki, 2018). Security infrastructure, intrusion prevention, and detection systems continue to evolve to mitigate security attacks such as social engineering attacks (Airehrour et al., 2018). When used alone, security tools have proven not to be effective in preventing the detrimental effects of social engineering (i.e., pretexting, phishing, baiting, and tailgating).

Respondents provided recommendations for the prevention of social engineering attacks. Most respondents recommended a user training and awareness program as the most effective strategy to prevent social engineering attacks. They most often described it using phrases like “most important” and “the primary technique.” Users become knowledgeable on social engineering techniques and appropriate ways of responding to an attack. P1 stated that “Training is the most important strategy. The workforce should be equipped with information on signs of an attack and how to deal with it.” P2 added a second recommendation for attack mitigation, stating the importance of installing and updating security controls, including firewalls, antivirus programs, strong passwords, and monitoring premises, specifying that IT managers should “secure your gadgets. Install and maintain up to date programs and firewalls.”

Cybersecurity incident simulation exercises. Respondents felt it was important for security teams to carry out drills, such as phishing simulations, to ensure users were familiar with frequent social engineering attacks, such as e-mail phishing, as well as penetration tests to identify weaknesses within the system.

Respondents recommended that security teams should carry out risk assessments mainly to identify and protect valuable assets. P6 added that “companies that actively seek to protect themselves from social engineering attacks often focus on securing most of its important assets from attackers.”

Formulating and enforcing security policies. Key among security policies are ones on the use of social media. Respondents recommended that policies limit disclosing too much personal and work-related information on social media platforms. P5 noted the importance of “having a good social media policy on privacy and posting. Educating the workforce on the importance of not sharing too much information.”

The final recommendation was backing-up data offsite. P3 noted that "implementing daily backups with a full backup conducted weekly should become standard practice. The backed-up data is then stored in a location outside of the organization's geographical area."

Theme 2: Training and Awareness

Respondents felt that technology executives should have risk assessment skills and, more particularly, be able to identify risks associated with their industries. Cybersecurity awareness programs and skills training are essential to the organization's protection from social engineering attacks (Adams & Makramalla, 2015). One way to obtain intelligence on industry-related security threats was by networking with security firms and information security experts in the same industry. P6 cited "technology skills are just keeping up to date with what's happening through organizations like Infragard, CIS, or any of the other alerting and monitoring agencies out there".

Risk mitigation skills were emphasized by all respondents as important to possess. Respondents felt technical executives should be able to detect suspicious activity such as malicious links and know-how to contain them. P5 gave the example to "reject any foreign offers since most of them are fake. Foreign offers include a lottery or sweepstake from unknown relatives". Besides intrusion detection, respondents also mentioned training skills, ability to put together a high performing security team as well as penetration testing skills.

Other skills mentioned by P4 include being subject matter experts and "understanding security in all different platforms and having the ability to develop security plans”. P3 described “developing a strong technology strategy which means learning what strategy means at the ground level and how to lead the times of technological change that comes from great ideas”.

The respondents felt that soft skills were the most critical skills for technology executives. For instance, they needed to have excellent communication skills to get the top management involved in cybersecurity issues as well as influence employee behavior. Interpersonal skills would enable technology executives to get along well with and influence staff at all levels, thereby shaping their behavior towards information security. P3 noted “having the ability to create and manage relationships with peers, coworkers, and others. Thus, getting your message through to people at all levels of the company with clarity”.

Technology executives need to have networking skills to enable them to create relationships and share threat-related information with people in the same industry. P5 explained that “technology executives should network by attending conferences and keeping up to date on security training”.

It is essential for technology executives to be approachable. Respondents felt that having an open-door policy would encourage employees to be open about any suspicious activities. P3 explained that executives “must seek to ensure their door is always open for conversations with employees. That way, employees feel free to report anything they may deem unimportant”.

Respondents felt that technology executives need to lead by example. P3 believes executives are likely to influence employees by modeling appropriate behavior “lead by example and champion security within the organization". P4 echoed similar sentiments regarding the importance of technology executives paying attention to detail "key to detail, to prioritize any small risks prompted in the organization". Finally, respondents felt that technology executives should have technical skills to manage social engineering threats effectively. P4 explained that "technical skills aid in predicting, detecting and preventing attacks".

Respondents highlighted that technology executives can champion data security policies was by developing security policies stipulating the processes and procedures to be followed in handling different security issues such as software and hardware devices, Internet protocol (IP) address configuration, and recovery responses. P1 stated that network services policies often dictate how the companies should handle certain issues, for example, IP address configuration.

Table 2

Training and Awareness

	Participant count	Document count
Importance of security awareness	6	4
Need for a strong security strategy	5	4

Assigning data security roles to all employees would increase the likelihood that they take ownership and become accountable for their actions. P6 emphasizes that "a company needs to ensure that it's staff in the information and technology sector, workforce, and management are aware of their responsibilities and what is expected of them”.

Technology executives should put systems in place to monitor account activities and assess the level of staff compliance with security procedures. P6 believes “the use of audits is a good way to ensure that the company’s staff and management are complying with the various elements of a data security policy”.

Identifying & containing risks. Respondents felt that technology executives should always be a step ahead by identifying vulnerable assets in the company and introducing measures to prevent attacks. P5 highlighted that “it is important to find any vulnerabilities in a company’s Information technology infrastructure before hackers do because hackers will scan for vulnerabilities the minute they are discovered”.

User training. Finally, technology executives ought to train staff to ensure that they are familiar with social engineering attacks and appropriate response strategies. P4 emphasizes that executives can “offer cybersecurity free training sessions in the office”.

Theme 3: IT Strategies

The strategies CISOs implement to mitigate these social engineering attacks need to continually evolve to keep up with sophisticated hacker attacks and the latest technology they have at their disposal. The inclusion of processes and policies specific to the business should be considered in addition to a customized IT strategy (Dawson, 2019). Respondents cited the importance of strategies and the ones they currently implement to prevent, detect, and respond to social engineering attacks, see Table 3.

Regarding user training and awareness, most respondents repeatedly mentioned people in terms of their actions and a sense of wanting to help. The sense of wanting to help implied that people in the company would be an easy target for cybercriminals. To prevent them from falling prey to these attacks, the respondents felt that it was essential to train and make them aware of the potential risks and how to manage them. P2 states that "when it comes to preventing, I always believe in self-awareness and training. Because some of these attacks are not complicated techniques, it is due to the small careless mistakes that people make".

There was also the recognition by respondents that social engineering techniques change rapidly, and hence the training should be frequent and ongoing. In support of training P6 added that "I think the people there need to be continuously reminded that we're always under attack, it's always changing, and here are the things to look out for, here's what we've seen in the last 30 days".

Table 3

Information Strategies

	Participant count	Document count
Importance of strategies	5	4
Customized strategy	6	4

Respondents engaged third parties to administer tests aimed at determining user awareness levels. P3 explains that "employees are tested by having an outside party conduct a social engineering test".

Ignoring suspicious emails. Respondents frequently talked about e-mails suggesting that threats were mainly engineered through e-mails. To prevent these attacks, respondents reported that they ignore and or delete unsolicited e-mails, e-mails in the spam folder, or e-mails that ask for sensitive information. P1 emphasized to “ignore any e-mails that are not expected or any messages asking for any confidential information and passwords”. Rejecting ‘request for help’ appeals. Another way in which criminals engineered attacks was through appealing to people’s sense of wanting to help, particularly during this period of COVID-19 pandemic. To prevent becoming victims, respondents said that they rejected such offers. P5 noted that employees should “reject requests for help or offers of help. This includes not accepting help from organizations that I do not have a relationship with”. They were installing and updating software. Respondents secured their computer devices by installing software such as antivirus, antimalware, Wireshark traffic analysis, and email scanning software.

Other approaches included hiring competent IT staff to stop attacks before they happen, using a multi-layered approach, performing regular data back-up offsite, and having a disaster and recovery plan and policies to guide responses to social engineering incidents. Finally, respondents emphasized the need to understand their industries to help them in identifying potential risks. P1 explained that IT staff have the responsibility to “understand the industry you’re in and what risks you’d typically face and your exposure”.

Planning and sticking to the plan were emphasized by the respondents. A few respondents felt that creating a plan well in advance was the most critical strategy.

However, it was not enough to have a plan; they needed to adhere to it. P6 stated “you don’t want to wait till it happens before you develop your plan. Once you have your plan put together, follow the adage of plan the work, and work the plan. Don't wing it, unless there's an obvious thing missing”.

Prior to any initial employee training, it is essential to identify priority areas. Social engineering campaign reports provide a good indication of these priority areas. P1 provides as an example of needs assessments “reporting on social engineering campaigns to identify additional training required”.

Training provides an opportunity for employees to familiarize themselves with organizational security policy and procedures, potential security risks such as ransomware, and essential security measures such as changing passwords frequently. The respondents were keen to caution that technology is very dynamic, as are social engineering techniques. As such, it was essential to have regular training to ensure that employees are up-to-date with the latest risks and to promote conformance. P5 stated that “repetition is a key step in forming a habit. Cybersecurity is continuously changing; hence continuous training is important since they will be equipped with the latest scams and how to deal with them”.

Besides theoretical-based training, practical training where employees are exposed to simulated attacks are essential as they allow employees to be able to recognize threats and know how to handle them. P1 lists “exercising live-fire training to test how the employee would react and deal with such a situation”.

Social engineering training should be targeted to all the company staff. Respondents reported that they integrated the training into onboarding programs so that new staff became familiar with security measures.

Other strategies included bringing in external experts to facilitate training as well as entrenching a training culture by identifying training champions. P5 described this as “appointing cybersecurity culture advocates”.

Development of a comprehensive cybersecurity framework. Some of the respondents had plans stipulating procedures to follow to manage and mitigate a social engineering attack. P1 highlighted the importance of “having the proper procedures in place to mitigate cybersecurity breaches”.

Fostering and sustaining a cybersecurity culture. Some respondents built a security culture by creating awareness of social engineering threats from the top management levels to the technical levels. P3 explained this as “fostering and sustaining a culture of security at all levels of the organization. Making people aware of how human behavior, not just technological failure, can be a threat”.

Limiting public information. Respondents warned employees against disclosing sensitive work-related information, which was likely to be leveraged by cybercriminals. P5 noted that “all the employees should be warned against posting out of office details. If an employee post that they are out of the country on the company website, the thieves could take advantage of the situation”.

Building effective communication channels. Respondents ensured they had the right channels of communication to allow information to flow easily and enable employees to report any attacks as well as suspicious activities. P4 explained this as ”implementing a clear communication channel for cybersecurity concerns”. A few mentioned that they used different modes of communication to verify the information. P1 noted this as “having more than one mode of communication to verify certain information. For example, cell phones or telephone lines”.

Common among all respondents was training employees. The training targeted all employees to familiarize them with potential security threats such as phone phishing (vishing) as well as ensuring that they developed appropriate response strategies such as resisting from entering personal information on unsecured websites. P3 added the importance of “training employees to recognize common types of social engineering and how these tactics could overwhelm standard controls”.

Implementing layered security. Respondents talked about having several layers of security ranging from (a) technical controls such as spam filters, antivirus software, and firewall, (b) user access controls such as multifactor authentication, (c) separation of duties to increase the probability of one person detecting suspicious activities, and (d) regular monitoring of online accounts to check for unauthorized transactions. They were also keen to keep updating security controls to ensure that they were effective against more recent threats. P2 highlighted that “since these assaults are on the ascent, various new methods have been implemented to prevent countless phishing attacks before they even arrive at the interior servers”.

Testing security controls. While it was essential to implement controls, respondents felt it was more important to test both the staff for compliance and all other controls for effectiveness. They stressed the need to have the testing done by an independent auditor. P3 added the importance of “periodically evaluating the internal controls and compliance, preferably using an independent auditor”.

A back-up data plan was a common component in the respondent’s contingency plan. Backing up data would protect against losing data and enable the restoration of operations following a security incidence. One respondent mentioned that they used flash disks for backing data. P6 explained that “the organization must have an effective backup plan in place to rapidly restore service following a cyber-attack’”

A business continuity plan was another component used by respondents to ensure that business processes continued to function amidst a security attack. P5 noted that “creating a business continuity plan is the implementation of a strategy to maintain business operations during a catastrophic event”.

Some respondents planned for continuous education to ensure that all the employees were familiar with social engineering risks and developed knowledge on how to handle them. P1 added that “there should be regular and continuous training for employees on social engineering and improved ways of dealing with situations”.

A few respondents said they had an incident response team in place and ensured that it was accessible for staff to report any incidents. P3 noted that the creation of an incident response plan should include “assigning an executive or business leader to oversee the disaster recovery plan, communicate between teams, and check in on various business units”.

A few respondents said they had plans to quarantine infected devices from the system to stop the spread of malware. They would also consider a shutdown of the entire system in severe cases. P4 added that ”if the attack is severe or unknown, shutting down the whole system is the last resort”.

Social engineering attacks are inevitable. Respondents were quick to caution that social engineering attacks were bound to happen, with P6 stating “it’s not going to be if we have a compromise; it’s going to be when”. Yet, the cost of the attacks is enormous. Organizations suffer financial losses, business disruption, and loss of reputation. P1 noted “effects of social engineering are huge losses from financial theft and fraud, reduced competitiveness due to the loss of information and major effects on society due to interruptions in businesses”.

Though inevitable, it is possible to prevent and or mitigate social engineering attacks. Respondents emphasized the need to develop and review plans detailing prevention measures and response procedures. However, it was not enough to have security plans; technical executives needed to lead the organizations in practicing the plans in simulated attacks. P6 noted that this involved “just making sure the organization has the plan ready, knows what the plan is, and ideally has practiced that at least once a year”.

Besides developing response plans, respondents recommended that the technology team be curious and keep up with the constantly changing security threats. P6 explained this as “doing their best to stay abreast of the changing dynamics of the social engineering attacks. It’s the most fluid piece of the cyber threat landscape right now, it’s so easy to change, so quickly”.

Given the dynamics of social engineering, the respondents felt it is essential that incidence response plans are flexible enough to accommodate changes. P3 described this as “scheduling regular reviews and updates to business continuity plans to accommodate the changing nature of technology and any changes in the organization’s strategy”.

Comparison of existing studies and research findings

The knowledge discussed in new peer-reviewed studies regarding strategies for social engineering attack mitigation is confirmed by the themes within the research findings.

IT risks. To protect operational stability within the organization, respondents sought to utilize risk management as a proactive component toward managing security risks. Similarly, Oates (2019) felt management and employees involved must understand the new organizational risks. This includes new attack vectors, attack methods, and attack plains that emerge with each new technology. In a study of 20 IT managers, risk managers, business continuity professionals, and executives, Yeboah-Afari (2020) found that the role of risk management in the IT sector was crucial, especially when it came to business continuity planning. This was confirmed by respondents who said the development and implementation of a cybersecurity risk management strategy were important for fostering a cybersecurity culture and mitigating security breaches. The findings confirmed that CISOs that were successful in mitigating social engineering attacks had a wealth of technical and managerial skills that fed into the risk management strategies they implemented. Without this careful balance of skills, CISOs would have failed to recognize attacks or convince employees to learn mitigation tactics. This sentiment aligns with Gutta (2019) who found many senior managers lack the competencies to implement an enterprise risk management system and align organizational resources such as people, processes, and technology to prevent cyberattacks on enterprise assets.

Security Awareness. The research findings on the importance of a security awareness program, correlated with a recent qualitative study by Oates (2019) which found employee interaction programs such as training and education, monitoring, separation of roles, and management involvement reduce security risks. Simpson (2019) noted a lack of awareness and understanding of policy as the cause of unauthorized information disclosures. He further adds that a lack of security awareness is rife in organizations as they tend to consider these programs inefficient or costly. Respondents highlighted the importance of a security awareness program. They further emphasized the inefficiencies of such a program are outweighed when the program is paired with other technical and formal controls. In 2018, the Center for Development of Security Excellence released findings that highlighted unauthorized disclosures of information that have occurred due to the lack of education and security awareness. Kostic (2020), found that an expanded suite of information security awareness was required in organizations to mitigate the increase in cybersecurity activity leading to significant financial losses.

IT Strategies. A study by Johnson (2019) found strategic alignment and strategy execution concerning information technology projects executed in the banking industry has an impact on operational effectiveness. This is emphasized by respondents that cite the importance of strategic development and successful implementation. Porterfield (2016) emphasized the importance of an IT strategy being needed due to the approaching advancement of threats. Porterfield added that cyber specialists need a better understanding to develop future improved risk strategies to promote a more precise knowledge about minimizing security risks in organizations. Hammond (2019) found that a practical and efficient risk management strategy encompassing information security awareness can have a positive effect on both user behavior and asset protection. This correlates with respondents that highlighted that the implementation of a balanced control strategy leads to effective IT practice and reduces intellectual property theft. In addition to discussing the importance of developing a balanced control strategy, respondents emphasized the importance of developing and implementing a strategy that is customized for their organization rather than one-size-fits-all. This is reflected by Dawson (2019), who stated that the inclusion of processes and policies specific to the business should be considered in addition to a customized IT strategy.

While the three themes discovered in the research study are confirmed by the new studies discussed, the overall strategy highlighted by the research findings of implementing a balanced control strategy through the inclusion of technical, formal, and informal controls largely extends the knowledge in this discipline.

Findings in relation to the conceptual framework

Dhillon’s balanced control theory is a conceptual framework used within this study to clarify details of employee behavior and organizational management systems associated with the research. The research findings confirmed the ideals of the balanced control theory, which states that the implementation of balanced technical systems, formal policies, and informal control strategies work to mitigate computer crime. The research themes illustrated the importance of clarifying details of employee behavior and organizational management systems associated with the research. The balanced control theory, developed by Dhillon in 1999, focuses on the implementation of balanced technical systems, formal policies, and informal control strategies to mitigate computer crime (Dhillon, Hong & Tejay, 2007). The stable control theory aims to implement control strategies that mitigate computer crime and abuse by employees. These control strategies are comprised of preventative measures such as supervision, to reduce the opportunity for a crime, and the creation of an environment that fosters a strong sense of moral conscience (Dhillon et al., 2007).

During data analysis, some keywords, such as attack techniques, training, and data backup, emerged in numerous themes. The research study's emergent themes reflected the balanced control theory ideals of balanced technical systems, formal policies, and informal control strategies. The importance of exploring successful social engineering mitigating strategies implemented by CISOs is that further emphasis on practices that integrate the balanced control theory may mitigate data breaches and prevent cyber-attacks. According to the FBI (2020), the collective impact is staggering. Billions of dollars are lost every year, repairing systems hit by such attacks. Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and 9-1-1 centers around the country.

Findings tied to the existing literature

IT risks. Risk management is the process whereby business risks are identified and used to develop a strategy that will detect, minimize, and respond to risks (Lin, Rivera, Abrahamsson, & Tehler, 2017). The first significant theme identified during the NVivo data analysis was the importance of identifying and managing technology risks and the use of various policies and procedures to prevent, limit, or respond to social engineering attacks. The research findings align with Njenga and Jordaan (2016), who stated that Information security executives within an organization should be knowledgeable regarding security risks that extend past technology. Information security risk management is an integral part of an organization's business strategy and risk mitigation as it protects information availability, integrity, and privacy (Amine, Mostafa, & Wissam, 2016). Respondents emphasized information security risk assessment as the core of information security. This sentiment is also tied to that of Adesemowo, Von Solms, and Botha (2016). They believed information security risk management has turned out to be an essential element of best practice in corporate governance. A concern among respondents was the challenges with keeping up with and thwarting the increasingly complex social engineering attacks. This challenge was also presented by Nazareth and Choi (2015). They stated that managing information security risks is both challenging and critically important, particularly given the increasing frequency, rapid evolution, and severity of threats to organizations.

Security Awareness. Most respondents recommended a user training and awareness program as the most effective strategy to prevent social engineering attacks.

Adams and Makramalla (2015) also believed cybersecurity awareness programs and skills training are essential to the organization’s protection from social engineering attacks. To prevent employees from falling prey to these attacks, the respondents felt that it was essential to train and make employees aware of the potential risks and how to manage them. In the same light, Bhardwaj and Goundar (2019) stated businesses conduct user awareness training on security vulnerabilities to educate employees on the risks and responsibilities of protecting information technology assets. Respondents felt it is important to include security awareness within an organization's strategy. This is also in line with sentiments by Cerveny, Sanders, and Woo (2018), who felt information security research has mostly paid less attention to the inclusion of both security culture and awareness in building a successful information system that mitigates social engineering attacks. Dobrolinsky (2015) emphasized the necessity of awareness training in influencing changes in human behavior. Similar to the findings, Safa et al. (2015) reasoned that people tend to be more protective when they know their financial data or personal data are at risk.

IT strategies. Respondents felt that information security strategies with a focus on technical, formal, and informal controls to mitigate social engineering attacks might lead to effective IT practice by reducing intellectual property theft and limiting unauthorized access to sensitive data, thereby safeguarding organizational resources. The findings are in line with Ani, He, and Tiwari (2016), who believe to be comprehensive, an IT strategy must be comprehensive, which includes up-to-date security practices. They add that this comprehensive strategy must include security solutions that enable employees to recognize cybersecurity concerns and react accordingly and appropriately are essential. Dhillon, Hong and Tejay (2007) made a similar argument by stating that rather than focus on specific information security strategies, a balanced information security strategy consisting of technical, formal, and informal controls would be more successful.

Applications to Professional Practice

The findings of this study, including the analysis of the conceptual framework and review of scholarly articles and peer-reviewed studies, add to the existing publicly available knowledge to improve the mitigation of social engineering attacks. There is a need for successful organizations to identify appropriate information security theories for managing an effective IT security program, which includes social engineering mitigation strategies (Lin, & Lu, & Kuo, 2017). The most significant contribution from the study findings may be the identification of successful strategies to mitigate social engineering attacks. Respondents highlighted the need to continue to fine-tune these strategies as these attacks change. Regardless, organizations tend to learn from both past failures and successes (Matthies & Coners, 2018).

The research study findings indicated successful CISOs effectively implement three significant strategies to safeguard their organizations from social engineering attacks. The most implemented technique across the board for all respondents consists of developing, implementing, and continually evaluating a comprehensive plan to assess information technology risks. The successful plans included (a) understanding manipulative techniques used by cybercriminals, (b) knowing the models for assessing information technology risks, (c) awareness of challenges to respond to social engineering attacks, (d) recommendations to prevent social engineering attacks.

The second implemented technique most frequently used successfully includes security awareness and training. Data analysis and scholarly articles highlighted the importance of security awareness training among employees and also upper management. All of the respondents in the research study reported the importance of security awareness training to protect organizations from ever-evolving social engineering attacks. The successful strategic plans included (a) management skills needed by technology executives, (b) technical skillsets needed by technology executives, and (c) championing by technology executives.

The third technique frequently implemented according to the research study and scholarly articles for successful mitigation of social engineering attacks is the creation, implementation, and evaluation of IT strategies. Existing literature has depicted primary defense strategies of technology controls utilized through hardware and software. Organizational strategies for mitigating these attacks through internal organization settings are lacking (Jayakar, 2018). There is a need for successful organizations to identify appropriate information security theories for managing an effective IT security program, which includes social engineering mitigation strategies (Lin, Lu, & Kuo, 2017). Management needs to be aware of business risks that may lead to failure and develop mitigation strategies to avoid a crisis. The strategies CISOs implement to mitigate these social engineering attacks need to continually evolve to keep up with sophisticated hacker attacks and the latest technology they have at their disposal. Anderson (2017) discussed the need for organization executives to have access to up to date information on emerging risks and risk mitigation strategies. The successful IT strategies listed across scholarly articles and confirmed by respondents as implemented are (a) employee training strategies, (b) risk management strategies, and (c) cyberattack contingency plan.

The application to professional practice is incorporated in the various communications of the successful strategies identified to protect their organizations against social engineering attacks. The research findings illustrate the application of successful strategies implemented by the CISOs. They may provide technology executives and industry leaders with a baseline guide to assess their vulnerabilities and mitigate social engineering attacks. The research findings align with the balanced control theory, which states that the implementation of balanced technical systems, formal policies, and informal control strategies work to mitigate computer crime.

Implications for Social Change

There are several implications for social change from this research study. One implication is the potential impact of successful social engineering mitigation strategies for technology leaders to prevent future attacks. A significant challenge facing CISOs is the ability to mitigate against constantly evolving social engineering attacks. The implementation of cybersecurity strategies, as discussed in the research study findings, provides technology executives with increased awareness of security methodologies to be implemented on an ongoing basis to mitigate social engineering attacks and enhance the protection of both organizational and consumer data. This qualitative multicase study fills a gap in the related literature by providing additional and more current perspectives on successfully mitigating social engineering attacks within a continually evolving technology-focused environment.

Findings from the study have provided technology executives with three major successful strategies to mitigate social engineering attacks (a) IT risks, (b) security awareness, and (c) IT strategies. The implementation of these strategies may enhance the protection of consumer data within the organizations' network, which may lead to an increase in consumer confidence and result in increased economic prosperity. The findings of this study may help leadership identify perceptions within the organizations on the implementation of education, training, procedures, processes, and policy. These findings may also be shared with other leaders and may transform the industry's view of social engineering strategies and enable leaders to mitigate these attacks in the future. Surviving these social engineering attacks may enable organizations to further affect economic growth by employing residents within their communities and thereby stimulating the socioeconomic lifecycle.

Research forms a critical foundation for programs that seek to engage communities in sustainable change. Without ongoing research, developed programs are more likely to be based on inferred needs within the community or assumed problem identification. The findings may also provide researchers with validated data that can be used for further studies in this field.

Recommendations for Action

Organizations need to implement cybersecurity policies that enable the mitigation of social engineering attacks. It is estimated that malicious cyber activity cost the U.S.

economy between $57 billion and $109 billion in 2016 (U.S. Council of Economic Advisors, 2018). In 2017, federal executive branch agencies reported 35,277 incidents to the U.S. Computer Emergency Readiness Team. These incidents included web-based attacks, phishing, and the loss or theft of computing equipment (U.S. Government Accountability Office, 2019). The FBI's Internet Crime Complaint Center received 467,361 complaints in 2019 – a daily average of 1,300 – and recorded more than $3.5 billion in losses to both individuals and organizations. The most frequently reported complaints were phishing and similar scams (FBI, 2020).

The findings of this research study indicate CISOs implement IT strategies to mitigate social engineering attacks such as (a) employee training strategies, (b) risk management strategies, and (c) cyberattack contingency plans. With the knowledge of a security strategy baseline used by CISOs to mitigate social engineering attacks, I recommend CISOs, technology executives' and organizations take into consideration the following actions to secure their information systems and enhance their cybersecurity practices:

1. Assess the cybersecurity health of the organization through the identification and evaluation of the industry and organizational risks; the identification of vulnerabilities their information assets have; the development of a strategy which will detect, minimize, and respond to business and system risks.
2. Create and implement a comprehensive cyberattack contingency plan, which provides instructions, recommendations, and considerations for a company on how to recover their IT services and data in the event of a security breach,

disaster or system disruption. Practices incorporated into the incident-response plan should look at a minimum include:

a. Assigning an executive or business leader to oversee the disaster recovery plan, communicate between teams, and check in on various business units.

b. Awareness training for the employees. There should be regular and continuous training for employees on social engineering and improved ways of dealing with situations. Thus, the employees gain knowledge on how to handle or escalate a social engineering situation.

c. Quarantining the infected device(s) or isolate the network to prevent the spread of malware.

d. Systems backup of essential data. This backup is to avoid data loss should a data breach occur.

e. Business continuity plan creation. This ensures that business operations continue even after an attack.

f. They are reporting incidents as per the cyber insurance policy to offset costs involved with recovery after a cyber-related security breach.

3. Development of a strategic cybersecurity plan. This strategic plan will include procedures to protect confidential data and at a minimum should include:

   a. The use of multifactor authentication:

      i. Something You Know – includes passwords, personal identification numbers, combinations, code words.

ii. Something You Have – includes all items that are physical objects, such as keys, smartphones, smart cards, USB drives, and token devices.

iii. Something You Are – includes any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification.

b. Installing reputable security software and knowing your security baseline.

c. We are conducting security assessments and social engineering programs through a 3rd party company.

d. We are employing end-to-end data encryption for secure data transmission.

The results of the study and recommendations will be supplied to the study participants via a summary fact sheet. I will conduct a lunch and learn at Visa Inc, a global payments technology company, to discuss my research findings and its relevance to organizations within the West Coast region. I will also provide consultancy services as a guest speaker at information security conferences and workshops focused on advisory services for small to medium-sized organizations. Lastly, I will seek opportunities to share my research studies through industry publications and academic journals.

Recommendations for Further Research

Cybercrime is on the rise, and social engineering attacks are becoming ever more sophisticated. Small to medium-sized organizations are susceptible to these social engineering attacks. The research findings and recommendations may contribute to current and future research focused on successful mitigation strategies to prevent social engineering attacks in organizations. This study was geographically limited to the West Coast region. I would recommend a future study based on an expanded or different geographical area to compare and contrast the research findings. In addition to a different geographical location, I would recommend an expanded sample size of the research participants. While I reached data saturation with my study sample size of six CISOs, an expanded sample size would determine if the results may vary based on different sample sizes.

A factor that may limit further research is finding CISOs in the West Coast region who are willing to participate in a research study. The amount of time spent identifying and successfully obtaining CISOs to participate in the research study, significantly increased the time it took to obtain research results and conduct analysis. I would recommend future researchers consider assigning additional time to schedule CISOs as research participants. Extending the study research participants pool to include IT security managers may offer varied information and insight.

Reflections

Completing the DIT program and especially the research study has been a long and rewarding process. I have gained significant knowledge of both cybersecurity attacks and strategies implemented successfully to mitigate social engineering attacks; correctly, those implemented by CISOs within the West Coast region. I am better placed than before to share mitigation strategies for social engineering attacks with organizations, scholars, and community leaders. The strategies, compiled from the research findings, may contribute to current and future research to determine best practices, organizations may use to protect their information assets and mitigate social engineering attacks.

Before conducting interviews with research participants, I was aware of the importance of mitigating bias by avoiding making assumptions and asking leading questions when conducting interviews with participants. A personal bias I held before conducting the interviews was that the majority of CISOs were either not aware of or did not enforce adequate social engineering mitigation strategies to address potential attacks. My experience in various cybersecurity roles for technology organizations enforcing successful cybersecurity strategies fueled this bias. As I came to discover during the research interviews, the CISOs each had a career of successful mitigation strategies within cybersecurity. They were all fully aware of constant technological advancements and the accompanying opportunities for attackers to take advantage of increasing vulnerabilities to leverage, and the subsequent effect of these vulnerabilities on the security of their data assets. As I conducted the interviews, I was aware not to make assumptions, ask leading questions, or react audibly to their responses. Through member checking, I am confident that the participants provided unreserved responses to the interview questions and were not influenced either way by any of my actions.

My personal bias has since been changed regarding CISOs and their attitudes toward strategies for mitigating social engineering attacks. My analysis conducted during the literature review leaned toward the hesitation of organizations to utilize third-party tools and vendors due to the high cost. Following the interviews and analysis of findings, I have come to realize that CISOs are not only open to the use of third-party vendors and tools, but they also encourage this method to evaluate their risks. CISOs interviewed emphasized the importance of conducting security assessments and social engineering programs through a third-party vendor. These vendors, the CISOs found, we are adaptable, able to offer services to scale, able to provide cost-effective infrastructure services, and limit overall the liabilities that organizations would face in case of a data breach.

Summary and Research Conclusions

This qualitative multiple case study explored successful strategies CISOs implement to mitigate social engineering attacks and protect their data assets. The findings form a security baseline for cybersecurity strategies that other organizations may use to mitigate social engineering attacks successfully. Findings from the study merged into three main themes that correlated with the literature review and conceptual framework of the balance control theory. The three major themes found across successful strategies to mitigate social engineering attacks are (a) IT risks, (b) security awareness, and (c) IT strategies. The implementation of these strategies may enhance the protection of consumer data within the organizations' network, which may lead to an increase in consumer confidence and result in increased economic prosperity. The constant technological advancements have led to the need for CISOs to protect their data assets through the development and implementation of cybersecurity best practices.

References

Abrahamsen, E. B., Aven, T., Pettersen, K., Kaufmann, M., & Rosqvist, T. (2017). A framework for the selection of a strategy for the management of security measures. *Journal of Risk Research, 20*(3), 404-417.

Achuthshankar, A., Achuthshankar, A., Arjun, K., & Sreenarayanan, N. (2016). Encryption of reversible data hiding for better visibility and high security. *Procedia Technology*, *25*, 216-223 http://dx.doi.org/10.1016/j.protcy.2016.08.100

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*, *2015*(1), 5-14. Retrieved from http://timereview.ca

Adesemowo, A. K., Von Solms, R., & Botha, R. A. (2016). Safeguarding information as an asset: Do we need a redefinition in the knowledge economy and beyond? *South African Journal of Information Management*, *18*(1), 1–12. http://dx.doi:10.4102/sajim.v18i1.706

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security,* 4227-4239. http://dx.doi.org/10.1016/j.cose.2014.01.001

Airehrour, D., Nair, N., & Madanian, S. (2018). Social engineering attacks and countermeasures in the New Zealand banking system: Advancing a user-reflective mitigation model. *Information, 9*(5), 2078–2489 http://dx.doi.org/10.3390/info9050110

Alazab, M. (2015). Profiling and classifying the behavior of malicious codes. *Journal of*

Systems and Software, *100*, 91-102. http://dx.doi.org/10.1016/j.jss.2014.10.031

Albuquerque, R., Villalba, L., Orozco, A., Júnior, R., & Kim, T. (2016). Leveraging information security & computational trust for cybersecurity. *Journal of Supercomputing*, *72*(10), 3729-3763.http://dx.doi.org/10.1007/s11227-015-1543-4

Alebrahim, A., Hatebur, D., Fassbender, S., Goeke, L., & Côté, I. (2015). A pattern-based and tool-supported risk analysis method compliant to ISO 27001 for cloud systems. *International Journal of Secure Software Engineering*, *6*(1), 24-46. http://dx.doi.org/10.4018/ijsse.2015010102

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. *European Journal of Information Systems*, *26*(6),661-687.http://dx.doi.org/10.1057/s41303-017-0057-y

Alkhoraif, A., Rashid, H., & McLaughlin, P. (2018). Lean implementation in small and medium enterprises: A literature review. Operations Research Perspectives. https://dx.doi.org/ 10.1016/j.orp.2018.100089

Almalki, S. (2016). Integrating quantitative and qualitative data in mixed methods research--Challenges and benefits. *Journal of Education and Learning*, *5*(3), 288–296.

Al-Yateem, N. (2012). The effect of interview recording on the quality of data obtained: A methodological reflection. Nurse Researcher. 19(4), 31-35. http://dx.doi.org/10.7748/nr2012.07.19.4.31.c9222

Ames, H., Glenton, C., & Lewin, S. (2019). Purposive sampling in a qualitative evidence synthesis: A worked example from a synthesis on parental perceptions of vaccination communication. *BMC Medical Research Methodology*, (1), 1. https://dx.doi.org./10.1186/s12874-019-0665-4

Amine, B., Mostafa, B., & Wissam, A. (2016). Improvement of information system security risk management. *2016 4th IEEE International Colloquium on Information Science and Technology (CiSt)* http://dx.doi.org/10.1109/CIST.2016.7805039

Amundrud, O., Aven, T., & Flage, R. (2017). How the definition of security risk can be made compatible with safety definitions. Proceedings of the Institution of Mechanical Engineers, Part O: *Journal of Risk and Reliability, 231*(3) 286 – 294. https://dx.doi.org/10.1177/1748006X17699145

Anderson, D. (2017). COSO ERM: Getting risk management right: Strategy and organizational performance are the heart of the updated framework. Internal Auditor. 74(5), 38-43.

Ani, U. P. D., He, H., & Tiwari, A. (2016). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology*, 1-43. http://dx.doi:10.1080/23742917.2016.1252211

Anleu, S. R., Blix, S. B., Mack, K., & Wettergren, Å. (2016). Observing judicial work and emotions: Using two researchers. Qualitative Research. 16(4), 375–391. https://dx.doi.org/10.1177/1468794115579475

Arhin, K., & Wiredu, G. O. (2018). An organizational communication approach to information security. *African Journal of Information Systems, 10*(4), 261–279.

Atoum, I., Otoom, A., & Ali, A. (2017). Holistic cybersecurity implementation frameworks: A case study of Jordan. *International Journal of Information, Business, and Management*, *9*(1), 108. https://www.academia.edu/32698394/International_Journal_of_Information_Business_and_Management

Atwell, C., Blasi, T., & Hayajneh, T. (2016). Reverse TCP and social engineering attacks in the era of big data. *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*. http://dx.doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.60

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 & Security. 66, 218–234. https://dx.doi.org/10.1016/j.cose.2017.02.006

Awad, A., Gill, S., Lee, B., Kadry, S., & Maddodi, G. (2016). Data leakage detection using system call provenance. *2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, 486, 2016.

Bakhshi, T. (2017). Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. *2017 13th International Conference on Emerging Technologies (ICET)*. http://dx.doi.org/10.1109/ICET.2017.8281653

Barafort, B., Mesquida, A., & Mas, A. (2018). Integrated for IT organizations based on ISO 31000 in an ISO multi-standards context. Computer Standards & Interfaces.

57-66. http://dx.doi/org/10.1016/j.csi.2018.04.010

Barczak, G. (2015). Publishing qualitative versus quantitative research. *Journal of Product Innovation Management, 32*(5), 658. http://dx.doi.org/10.1111/jpim.12277

Barkham, A. M., & Ersser, S. J. (2017). Supporting self-management by community matrons through a group intervention: An action research study. Health & Social Care in the Community. 25(4), 1337–1346. https://dx.doi.org/10.1111/hsc.12434

Barnham, C. (2015). Quantitative and qualitative research. *International Journal of Market Research, 57*(6), 837–854. https://dx.doi.org/10.2501/IJMR-2015-070

Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity taking off the blindfold. Field Methods. 27, 3-21. http://dx.doi.org/10.1177/1525822X14526838

Barrow, C. (2016). Leadership and management of orthodontic teams: Global perspectives and principles that never fail. Seminars in Orthodontics. 22, 251–261. https://dx.doi.org/10.1053/j.sodo.2016.08.004

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. Information & Management. 51, 138-151. http://dx.doi.org/10.1016/j.im.2013.11.004

Beebe, N., & Rao, V. (2005). *Using situational crime prevention theory to explain the effectiveness of information systems security, Proceedings of the 2005 Software's conference*, Las Vegas, NV, 10.

Belov, E., Los, V., & Malyuk, A. (2018). The digital economy and actual problems of the improvement of the training system in the field of information security. Bezopasnostʹ Informacionnyh Tehnologij. 25(4) 6-22 https://dx.doi.org/10.26583/bit.2018.4.01

Benoit, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology*, 16, 21. http://dx.doi.org/10.1186/s12874-016-0114-6

Bergin, M. (2011). NVivo 8 and consistency in data analysis: Reflecting on the use of a qualitative data analysis program. Nurse Researcher. 18(3), 6-12. http://dx.doi.org/10.7748/nr2011.04.18.3.6.c8457

Bhardwaj, A., & Goundar, S. (2019). A framework to define the relationship between cybersecurity and cloud performance. Computer Fraud & Security, 2019(2), 12-19. http://dx.doi.org/10.1016/S1361-3723(19)30020-X

Bobitan, R., & Stefea, P. (2015). Integrated reporting - a more holistic picture for a company. Annals of The University of Oradea, Economic Science Series. 24(2), 448-456.

Bölte, S. (2014). The power of words: Is qualitative research as important as quantitative research in the study of autism? Autism. 18(2), 67-68. http://dx.doi.org/10.1177/1362361313517367

Bowden, C., & Galindo-Gonzalez, S. (2015). Interviewing when you’re not face-to-face: The use of email interviews in a phenomenological study. *International Journal* *of Doctoral Studies 10*, 79-92. Retrieved from http://ijds.org/Volume10/IJDSv10p079-092Bowden0684.pdf

Boyle, L. H., Whittaker, T. A., Eyal, M., & McCarthy, C. J. (2017). What really happens in quantitative group research? Results of a content analysis of recent quantitative research in JSGW. *Journal for Specialists in Group Work, 42*(3), 243–252. https://dx.doi.org/10.1080/01933922.2017.1338812

Braga, D., Niemann, M., Hellingrath, B., & Neto, F. (2019). Survey on computational trust and reputation models. ACM Computing Surveys (CSUR). 51(5). http://dx.doi.org/10.1145/3236008

Breach Level Index. (2018). Data breach database. Retrieved from https://breachlevelindex.com/

Brédart, A., Marrel, A., Abetz-Webb, L., Lasch, K., & Acquadro, C. (2014). Interviewing to develop patient-reported outcome (PRO) measures for clinical research: Eliciting patients' experience. Health and Quality of Life Outcomes. 12(1), 1-10. http://dx.doi.org/10.1186/1477-7525-12-15

Brewer, R. (2016). Ransomware attacks: Detection, prevention, and cure. Network Security. 2016(9), 5-9. http://dx.doi.org/10.1016/S1353-4858(16)30086-1

Brožová, H., Šup, L., Rydval, J., Sadok, M., & Bednar, P. (2016). Information security management: ANP based approach for risk analysis and Decision Making. Agris on-line Papers in Economics & Informatics. 8(1), 13–24. https://dx.doi.org/10.7160/aol.2016.080102

Bullée, J. W. H., Montoya, L., & Pieters, W. (2015). The persuasion and security awareness experiment: Reducing the success of social engineering attacks. http://dx.doi.org/10.1007/s11292-014-9222-7

Bureau of Labor Statistics. (2016). Business employment dynamics. Retrieved from https://www.bls.gov/bdm/entrepreneurship/entrepreneurship.htm

Burkus, D. (2015). Style theory. Retrieved from http://davidburkus.com/2010/02/style-theory

Burnap, P., French, R., Turner, F., & Jones, K. (2018). Malware classification using self-organizing feature maps and machine activity data. Computers & Security, 73, 399-410. http://dx.doi.org/10.1016/j.cose.2017.11.016

Calverley, D., Foulds, C., Nordhagen, S., O'Keefe, L., & Xinfang, W. (2014). Climate change research and credibility: Balancing tensions across professional, personal, and public domains. Climate Change. 125(2). https://dx.doi.org/ 10.1007/s10584-014-1167-3

Carlton, M., & Levy, Y. (2017). Cybersecurity skills: Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management, 5*(2), 16–28. Retrieved from http://www.iiakm.org/ojakm/articles/2017/volume5_2/OJAKM_Volume5_2pp16-28.pdf

Carolan, C. M., Forbat, L., & Smith, A. (2016). Developing the DESCARTE model: The design of case study research in health care. Qualitative Health Research. 26(5), 626–639. https://dx.doi.org/10.1177/1049732315602488

Castleberry, A. (2014). NVivo 10 [software program]. Version 10. QSR international;

2012. *American Journal of Pharmaceutical Education*, *78*, 25. http://dx.doi.org/10.5688/ajpe78125

Center for Development of Security Excellence. (2018). Insider threat case studies. Retrieved from: https://www.cdse.edu/resources/case-studies/insider-threat.html

Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24-41. http://dx.doi.org/10.1016/j.future.2015.09.031

Checkland, P. (2012). Four conditions for serious systems thinking and action. Systems Research & Behavioral Science. 29, 465-469. http://dx.doi.org/10.1002/sres.2158

Chiumento, A., Khan, M. N., Rahman, A., & Frith, L. (2015). Managing ethical challenges to mental health research in post-conflict settings. Developing world bioethics. 16, 15-28. http://dx.doi.org/10.1111/dewb.12076

Cho, J. Y., & Lee, E. (2014). Reducing confusion about grounded theory and qualitative content analysis: Similarities and differences. The Qualitative Report. 19, 1-20. Retrieved from http://nsuworks.nova.edu

Cody, A., Orebaugh, A., Scarfone, K., & Souppaya, M. (2008). Technical guide to information security testing and assessment. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Comia, H. (2017). Social engineering: Exploring social engineering toolkits. http://dx.doi.org/10.13140/RG.2.2.25074.30401.

Comley-White, N., & Potterton, J. (2018). The perceived barriers and facilitators in completing a master’s degree in Physiotherapy. *South African Journal of Physiotherapy, 74*(1), 1-5. http://dx.doi.org/10.4102/sajp.v74i1.445

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

Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. Oncology Nursing Forum. 41, 89-91. http://dx.doi:10.1188/14.ONF.89-91

Cope, D. G. (2015). Case study research methodology in nursing research. oncology nursing forum. 42(6), 681–682. https://dx.doi.org/10.1188/15.ONF.681-682

Cordell, N. (2015). More control, less risk. IT NOW. 57(2), 26-27. http://dx.doi.org/10.1093/itnow/bwv039

Cruz, E. V., & Higginbottom, G. (2013). The use of focused ethnography in nursing research. Nurse Researcher. 20(4), 36-43. http://dx.doi.org/10.7748/nr2013.03.20.4.36.e305

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. Behaviour & Information Technology, 37(1), 50-65. http://dx.doi.org/10.1080/0144929x.2017.1397193

Cullen, A., & Armitage, L. (2016a). The social engineering attack spiral (SEAS). *2016 international conference on cybersecurity and protection of digital services* *(cybersecurity)*. http://dx.doi.org/10.1109/cybersecpods.2016.7502347

Culver, D. M., Gilbert, W., & Sparkes, A. (2012). Qualitative research in sport psychology journals: The next decade 2000-2009 and beyond. Sport Psychologist. 26, 261-281. Retrieved from http://journals.humankinetics.com/tsp

Cunliffe, A., & Karunanayake, G. (2013). Working within hyphen-spaces in ethnographic research. Organizational research methods. http://dx.doi.org/10.1177/1094428113489353.

Dara Security. (2015, May). Quid pro quo: What is the cost of a free gift? Retrieved from https://www. Darasecurity.com/article.php?id=38

da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security. 49, 162–176. https://dx.doi.org/10.1016/j.cose.2014.12.006

Dawson, A. (2019). Exploring strategies for implementing information security training and employee compliance practices. *Walden Dissertations and Doctoral Studies*. 7794. https://scholarworks.waldenu.edu/dissertations/7794

Department of Homeland Security. (2018). Computer emergency response team (DHS US-CERT). Retrieved from www.us-cert.gov/index.html

Dhillon, G., & Moores, S. (2001). Computer crimes: Theorizing about the enemy within. Computers & Security, 20(8), 715-723.

Dhillon, G., Tejay, G., & Hong, W. (2007). Identifying governance dimensions to evaluate information systems security in organizations. Paper presented at the

40th Hawaii International Conference on System Sciences. Retrieved from https://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550157b.pdf

Dobrolinsky, K. (2015). Tips to combat the top three risk trends for schools. Education Digest, 81, 21-25. Retrieved from https://www.eddigest.com

Edwards, C. (2014). Researchers probe security through obscurity. Communications of the ACM. 57(8), 11-13. http://dx.doi.org/10.1145/2632038

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analyzing online social engineering attack surfaces. Computers & Security. 6918-34. http://dx.doi.org/10.1016/j.cose.2016.12.013

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis. SAGE Open. 4(1), 1-10. http://dx.doi.org/10.1177/2158244014522633

Faisal, W., & Maaruf, A. (2018). Hardening Cisco devices based on cryptography and security protocols - part one: Background theory. Annals of Emerging Technologies in Computing. 2(3) 27-44

Farrell, R. (2016). Cybersecurity analysis -- where "Life experience application" counts most. ISSA Journal. 14(5), 7-44.

Fatna, N. M., Younes, I., & Habiba, C. (2017). A security approach based on honeypots: Protecting the online social network from malicious profiles. Advances in Science, Technology, and Engineering Systems. 2(3), 198-204. http://dx.doi.org/10.25046/aj020326

Federal Bureau of Investigation. (2018). Internal crime report. Retrieved from https://pdf.ic3.gov/2018_IC3Report.pdf

Federal Bureau of Investigation. (2020). Internal crime report. Retrieved from https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

Federal Trade Commission. (2018). Consumer information. Phishing. Retrieved from https://www.consumer.ftc.gov/articles/0003-phishing

Fellnhofer, K. (2018). Game-based entrepreneurship education: impact on attitudes, behaviors, and intentions. World Review of Entrepreneurship, Management, and Sustainable Development, 14, 205-228. http://dx.doi.org/10.1504/WREMSD.2018.089066

Feng, Y., Hori, Y., & Sakurai, K. (2017). A behavior-based online engine for detecting distributed cyber-attacks. Lecture Notes in Computer Science. https://dx.doi.org/10.1007/978-3-319-56549-1_7

Ferrer, S., & Ruiz, T. (2017). The impact of the built environment on the decision to walk for short trips: Evidence from two Spanish cities. Transport Policy. https://dx.doi.org/10.1016/j.tranpol.2017.04.009

Foley, D., & O'Conner, A. J. (2013). Social capital and networking practices of indigenous entrepreneurs. *Journal of Small Business Management, 51*, 276-296. http://dx.doi.org/10.1111/jsbm.12017

Furnell, S., & Vasileiou, I. (2017). Feature: Security education and awareness: Just let them burn? Network Security. 2017, 5–9. https://dx.doi.org/10.1016/S1353-4858(17)30122-8

Fusch, P., & Ness, L. (2015). Are we there yet? Data saturation in qualitative research.

The Qualitative Report, 2015. 20(9). 1408-1416. Retrieved from http://www.nova.edu/ssss/QR/QR20/9/fusch1.pdf

García, J. A. T., Skotnicka, A. G., & Zamora, D. T. (2015). The new technology-based firm profile required for delimitation of its definition in empirical studies. *International Journal of Engineering Management and Economics, 5*(1-2), 114 128. http://dx.doi.org/10.1504/IJEME.2015.069903

Gendron, Y., Brivot, M., & Guénin-Paracini, H. (2015). The construction of risk management credibility within corporate boardrooms. European Accounting Review. 1-30. http://dx.doi.org/10.1080/09638180.2015.1064008

Gentles, S., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. Qualitative Report. 20(11), 1772-1789. Retrieved from http://nsuworks.nova.edu

Georgiou, A., Marks, A., Braithwaite, J., & Westbrook, J. I. (2013). Gaps, disconnections, and discontinuities - The role of information exchange in the delivery of quality long-term care. The Gerontologist. 53, 770-779. http://dx.doi.org/10.1093/geront/gns127

Georgiou, D., & Lambrinoudakis, C. (2017). Security policy rules and required procedures for two crucial cloud computing threats. *International Journal of Electronic Governance, 9*, 385-403. http://dx.doi.org/10.1504/IJEG.2017.088217

Gill, M. (2014). The possibilities of phenomenology for organizational research. Organizational research methods, 17(2), 118-137. http://dx.doi.org/10.1177/1094428113518348

Goodman-Delahunty, J., Martschuk, N., & Dhami, M. K. (2014). Interviewing high-value detainees: Securing cooperation and disclosures. Applied Cognitive Psychology. 28, 883-897. http://dx.doi.org/10.1002/acp.3087

Greavu-Şerban, V., & Şerban, O. (2014). Social engineering a general approach. Informatica Economica. 18(2), 5-14. http://dx.doi.org/10.12948/issn14531305/18.2.2014.01

Güngör, S. K., & Özkara, F. (2017). A qualitative research on administration ethics at school. *Journal of Education and Training Studies, 5*(11), 44–55. http://redfame.com/journal/index.php/jets/article/view/2705

Gutta, R. R. (2019). Managing security objectives for effective organizational performance information security management. *Walden Dissertations and Doctoral Studies. 7147*. https://scholarworks.waldenu.edu/dissertations/7147

Hadnagy, C. (2014). *Unmasking the social engineer: The human element of security*. Indianapolis IN: John Wiley & Sons, Inc.

Hammond, S. T. (2019). *Threat and coping appraisals on information security awareness training effectiveness: A quasi-experimental study* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No.22585443)

Harper, M., & Cole, P. (2012). Member checking: Can benefits be gained similar to group therapy? The Qualitative Report. 17, 510-517. Retrieved from http://www.nova.edu/ssss/QR/

Harrison, J. S., Banks, G. C., Pollack, J. M., O'Boyle, E. H., & Short, J. (2014).

Publication bias in strategic management research. *Journal of Management.* http://dx.doi.org/10.1177/0149206314535438

Harvey, L. (2015). Beyond member-checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education, 38*(1), 23–38.

Hatice, Y., Seref, S., & Yavuz, C. (2017). A Turkish language-based data leakage prevention system. (2017). 2017 5th International symposium on digital forensic and security (ISDFS). http://dx.doi.org/10.1109/ISDFS.2017.7916514

Hays, D. G., Wood, C., Dahl, H., & Kirk-Jenkins, A. (2016). Methodological rigor in Journal of Counseling & Development qualitative research articles: A 15-year review. *Journal of Counseling & Development, 94*, 172-183. http://dx.doi.org/10.1002/jcad.12074

Heartfield, R., & Loukas, G. (2017). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers & Security. 76, 101-127.

Henshel, D., Cains, M., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cybersecurity risk assessment. Procedia Manufacturing. 1117-1124. http://dx.doi.org/10.1016/j.promfg.2015.07.186

Hermanowicz, J. C. (2013). The longitudinal qualitative interview. Qualitative Sociology. 36, 189-208. http://dx.doi.org/10.1007/s11133-013-9247-7

Hoffman, H., & Sollner, M. (2014). Incorporating behavioral trust theory into system development for ubiquitous applications. Personal Ubiquitous Comput. 18(1), 117

128. http://dx. Doi.org/10.1007

Horne, C., Maynard, S., & Ahmad, A. (2017). Organizational information security strategy: Review, discussion, and future research. *Australasian Journal of Information Systems, 21*. https://dx.doi.org/10.3127/ajis.v21i0.1427

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case study research. Nurse Researcher. 20(4), 12-17. http://dx.doi.org/10.7748/nr2013.03.20.4.12.e326

Houghton, C., Murphy, K., Shaw, D., & Casey, D. (2015). Qualitative case study data analysis: An example from practice. Nurse Researcher. 22(5), 8-12. http://dx.doi.org/10.7748/nr.22.5.8.e1307

Houser, W. (2015). Could what happened to Sony happen to us? IT Professional. 17(2), 54-57. http://dx.doi.org/10.1109/MITP.2015.21

Hu, X., Xu, M., Xu, S., & Zhao, P. (2017). Multiple cyber-attacks against a target with observation errors and dependent outcomes: Characterization and optimization. Reliability Engineering & System Safety, 159, 119-133. http://dx.doi.org/10.1016/j.ress.2016.10.025IEEE. (2018).

IEEE. (2018). Cyber stealth attacks in critical information infrastructures. *IEEE Systems Journal* (2), 1778. http://dx.doi.org/10.1109/JSYST.2015.2487684

Internal Revenue Service. (2018). Newsroom. Don’t take the bait; avoid phishing and malware to protect your personal data. Retrieved from https://www.irs.gov/newsroom/dont-take-the-bait-avoid-phishing-and-malware-to-protect-your-personal-data

International Information System Security Certification Consortium. (2016). Report the state of cybersecurity from the federal cyber executive perspective. Key Findings. Retrieved from https://www.isc2.org/-/media/ISC2/Documents/ISC2-Federal-Cyber-Survey-report.ashx

International Organization for Standardization. (2018). About ISO. Retrieved from https://www.iso.org/about-us.html

Ionescu, C., Ceaușu, I., & Ilie, C. (2018). Considerations on the implementation steps for an information security management system. Proceedings of the International Conference on Business Excellence. 12(1) 476-485. https://dx.doi.org/10.2478/picbe-2018-0043

Izci, E., & Göktas, Ö. (2017). Assessment of in-service training activities for junior high mathematics teachers. Educational Research and Reviews. 12(24), 1220–1229. https://files.eric.ed.gov/fulltext/EJ1164618.pdf

Jackson, R. A. (2018). Pulling strings. Internal Auditor. 75(4), 34-39. Retrieved from https://rauschadvisory.com/downloads/ia201807-dl.pdf

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, *5*, 87-88. http://dx.doi.org/10.4103/0976-0105.141942

Janghorban, R., Roudsari, R. L., & Taghipour, A. (2014). Skype interviewing: The new generation of the online synchronous interview in qualitative research. *International Journal of Qualitative Studies on Health and Well-Being*. http://dx.doi.org/10.3402/qhw.v9.24152

Jayakar, K. (2018). Universal broadband: Option, right, or obligation. *Journal of Human Values, 24*(1), 11-24. http://dx.doi.org/10.1177/0971685817733569

Jedynak, P., & Bąk, S. (2018). The global risk landscape - its shape, tendencies, and consequences for management. *Journal of Economics & Management, 32*(2), 48-59. http://dx.doi.org/10.22367/jem.2018.32.04

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems, 34*(2), 597-626. http://dx.doi.org/10.1080/07421222.2017.1334499

Jiang, H., Zhao, S., Zhang, Z., & Yi, Y. (2018). Exploring the mechanism of technology standardization and innovation using the solidification theory of binary eutectic alloy. Technological Forecasting & Social Change. 135, 217–228. https://dx.doi.org/10.1016/j.techfore.2017.08.015

Johnson, A. A. (2019). *Strategic alignment and information technology projects in the banking industry* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 13806116)

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective in preventing social engineering attacks. Computers in Human Behavior. 75. https://dx.doi.org/10.1016/j.chb.2016.09.012

Kaczynski, D., Salmona, M., & Smith, T. (2013). Qualitative research in finance. *Australian Journal of Management, 39*(1), 127-135. http://dx.doi.org/10.1177%2F0312896212469611

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. Information and Computer Security. 25(3) 300-329, https://doi.org/10.1108/ICS-02-2016-0013

Keating, J., & Nourbakhsh, I. (2018). Teaching artificial intelligence and humanity. Communications of the ACM. 61(2), 29-32. http://dx.doi.org/10.1145/3104986

Kedgley, M. (2015). Feature: Security breaches – hiding in plain sight. Computer Fraud & Security. 7–9. https://dx.doi.org/10.1016/S1361-3723(15)30074-9

Kennedy, J. P. (2015). Losing control: A test of containment theory and ethical decision making. International Journal of Criminal Justice Sciences. 10(1), 48–64. http://www.sascv.org/ijcjs/pdfs/kennedyijcjs2015vol10issue1.pdf

Kim, B., Kim, K., Hong, S., & Oh, S. (2017). Development of cyber information security education and training system. Multimedia tools and applications. 76(4), 6051-6064. http://dx.doi.org/10.1007/s11042-016-3495-y

King, Z., Henshel, D., Flora, L., Cains, M., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Frontiers in Psychology. http://dx.doi.org/10.3389/fpsyg.2018.00039/full

Knobloch, M. J., Thomas, K. V., Patterson, E., Zimbric, M. L., Musuuza, J., & Safdar, N. (2017). Major article: Implementation in the midst of complexity: Using ethnography to study healthcare-associated infection prevention and control. *AJIC: American Journal of Infection Control, 45*, 1058–1063. https://dx.doi.org/10.1016/j.ajic.2017.06.024

Koçyigit, M. (2017). The meaning of marriage according to university students: A phenomenological study. Educational Sciences: Theory and Practice. 17(2), 679–711.

Komisar, V., Novak, A. C., & Haycock, B. (2017). Full-length article: A novel method for synchronizing motion capture with other data sources for millisecond-level precision. Gait & Posture. 51, 125–131. https://dx.doi.org/10.1016/j.gaitpost.2016.10.002

Korstjens, I., & Moser, A. (2017). Series: Practical guidance to qualitative research. Part 2: Context, research questions, and designs. *The European Journal of General Practice, 23*(1), 274–279. https:/dx.doi.org/10.1080/13814788.2017.1375090

Kostic, L. C. (2020). *Information security awareness techniques that reduce data breaches caused by social engineering attacks* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 27832769).

Kourti, I. (2016). Using personal narratives to explore multiple identities in organizational contexts. Qualitative research in organizations and management. 11(3), 169-188. http://dx.doi.org/10.1108/QROM-02-2015-1274

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22,* 113–122. https://dx.doi.org/10.1016/j.jisa.2014.09.005

Kuo, S. Y., Lin, P. C., & Lu, C. S. (2017). The effects of dynamic capabilities, service capabilities, competitive advantage, and organizational performance in container shipping. Transportation Research Part A: Policy and Practice, 95, 356-371. http://dx.doi.org/10.1016/j.tra.2016.11.015

Kwong, J. P., Kwong, E. J., Posluns, E. C., Fitch, M. I., McAndrew, A., & Vandenbussche, K. A. (2014). The experiences of patients with advanced head and neck cancer with a percutaneous endoscopic gastrostomy tube: A qualitative descriptive study. Nutrition in Clinical Practice. 29, 526-533. http://dx.doi.org/10.1177/088453361453269

Lanaj, K., Johnson, R. E., & Lee, S. M. (2016). Benefits of transformational behaviors for leaders: A daily investigation of leader behaviors and need fulfillment. *Journal of Applied Psychology*, *101*(2), 237–251. https://dx.doi.org/10.1037/apl0000052

Laskowski, P. (2017). Internet security – technology and social awareness of the dangers. Studies in Logic, Grammar, and Rhetoric. 50(1) 239-252. http://dx.doi.org/10.1515/slgr-2017-0027

Lee, S., Lee, S. G., & Yoo, S. (2003). An integrative model of computer abuse based on social control and general deterrence theories. Information & management, 41(2004), 707-708. http://dx.doi.org/10.1016/j.im.2003.08.008

Lekaj, E., & Kercini, D. (2017). The process of risk management for e-business. *Academic Journal of Business, Administration, Law & Social Sciences, 3*(2), 81-85.

Leppink, J. (2017). Revisiting the quantitative–qualitative-mixed methods labels: Research questions, developments, and the need for replication. *Journal of Taibah University Medical Sciences*. http://dx.doi.org//10.1016/j.jtumed.2016.11.008

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. Health Promotion Practice. 16, 473-475. http://dx.doi.org/10.1177/1524839915580941

Li, Q., Liu, X., & Sonali, C. (2017). Social engineering and insider threats. *International conference on cyber-enabled distributed computing and knowledge discovery (CyberC)*. http://dx.doi.org/10.1109/CyberC.2017.91

Lin, L., Rivera, C., Abrahamsson, M., & Tehler, H. (2017). Communicating risk in disaster risk management systems—Experimental evidence of the perceived usefulness of risk descriptions. *Journal of Risk Research, 20*(12), 1534-1553. http://dx.doi.org/10.1080/13669877.2016.1179212

Lips-Wiersma, M., & Mills, A. J. (2014). Understanding the basic assumptions about human nature in workplace spirituality beyond the critical versus positive divide. *Journal of Management Inquiry*, *23*, 148-161. http://dx.doi.org/10.1177/1056492613501227

Lord, N. (2018). Data insider. What is social engineering? Defining and avoiding common social engineering threats. Retrieved from https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats

Madsen, A. K. (2013). Virtual acts of balance: Virtual technologies of knowledge management as co-produced by social intentions and technical limitations. *Electronic Journal of E-Government, 11*, 183-197. Retrieved from http://www.ejeg.com/main.html

Manoj, S. K. A., & Bhaskari, D. L. (2016). Cloud forensics-A framework for investigating cyber-attacks in a cloud environment. Procedia Computer Science. 2016 (85), 149-154. http://dx.doi.org/10.1016/j.procs.2016.05.202

Mansfield-Devine, S. (2017). Feature: Bad behavior: exploiting human weaknesses. Computer Fraud & Security, 201717-20. http://dx.doi.org/10.1016/S1361-3723(17)30008-8

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. Business Horizons. 59, 257-266. http://dx.doi/org10.1016/j.bushor.2016.01.002

Maree, J. E., Parker, S., Kaplan, L., & Oosthuizen, J. (2016). The information needs of South African parents of children with cancer. *Journal of Pediatric Oncology Nursing, 33*, 9-17. http://dx.doi.org/10.1177/1043454214563757

Markelj, B., & Bernik, I. (2015). The safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications, 20*, 84-89. http://dx.doi.org/10.1016/j.jisa.2014.11.001

Marshall, C., & Rossman, B. G. (2010). *Designing qualitative research*. Thousand Oaks, CA: Sage Publications, Inc.

Martin, C. E., & Meyer, W. J. H. (2012). Organizational and behavioral factors that influence knowledge retention. *Journal of Knowledge Management, 16*, 77-96.

Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management, 34*, 1-13. http://dx.doi.org/10.1016/j.ijinfomgt.2013.06.002

Matthies, B., & Coners, A. (2018). Double-loop learning in project environments: An implementation approach. Expert systems with applications, 96, 330-346. http://dx.doi.org/10.1016/j.eswa.2017.12.012

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative, or mixed methods and choices based on the research. Perfusion. 30, 537-542. http://dx.doi.org/10.1177/0267659114559116

McKim, C. (2015). The value of mixed methods research: a mixed-methods study. *Journal of Mixed Methods Research, 11*(2), 202-222. http://dx.doi.org/ 10.1177/1558689815607096

McKim, V. L. (2017). Operational risk assessment. *Journal of Business Continuity & Emergency Planning, 10*(4), 339-352. http://dx.doi.org/10.1108/13673271211198954

Merriam, S. B. (2014). *Qualitative research: A guide to design and implementation*. San Francisco, CA: John Wiley & Sons.

Mironela, P. (2017). Considerations on preventing social engineering over the internet. Memoirs of The Scientific Sections of the Romanian Academy. 11, 85-96

Moghimi, M., & Varjani, A. Y. (2016). New rule-based phishing detection method. Expert systems with applications. 2016(53), 231-242. http://dx.doi.org/10.1016/j.eswa.2016.01.028

Moldes, C. (2018). Insider threat and the malicious insider threat. *Journal of Cyber Security and Information Systems, 6* (1). https://www.csiac.org/journal-article/compliant-but-not-secure-why-pci-certified-companies-are-beingbreached/

Morgan, D. L. (2019). Commentary—after triangulation, what next? *Journal of Mixed Methods Research, 13*(1), 6. https://dx.doi.org/10.1177/1558689818780596

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates, and scenarios. Computers & Security. 59, 186. http://dx.doi.org/178776230414872

Nadal, K. L., Davidoff, K. C., Davis, L. S., Wong, Y., Marshall, D., & McKenzie, V. (2015). A qualitative approach to intersectional microaggressions: Understanding the influences of race, ethnicity, gender, sexuality, and religion. Qualitative Psychology. 2, 147-163. http://dx.doi.org/10.1037/qup0000026

National Institute of standards and technology. (2018). The five functions. Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework/online-learning/five-functions

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. Information & Management, 52(1), 123–134. http://dx.doi:10.1016/j.im.2014.10.009

Nishigaki, M. (2018). Humanics information security. Concurrency and Computation: Practice and Experience, 30(2). http://dx.doi.org/10.1002/cpe.4274

Njenga, K., & Jordaan, P. (2016). We want to do it our way: The neutralization approach to managing information systems security by small businesses. *The African Journal of Information Systems, 8*(1), 3. 42-63. http://digitalcommons.kennesaw.edu/ajis/

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. Evidence-Based Nursing, 18, 34-35. http://dx.doi.org/10.1136/eb-2015-102054

Oates, J. (2019). *A qualitative grounded theory study of employee interventions to improve information security in small businesses* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 22615268).

Onwuegbuzie, J. A., & Hwang, K. (2014). Qualitative analysis techniques for the review of the literature. The Qualitative Report, 17, 1-28. Retrieved from http://www.nova.edu/ssss/QR/

Otto, B. (2015). Quality and value of the data resource in large enterprises. Information Systems Management. 32(3), 234-251. http://dx.doi.org/10.1080/10580530.2015.1044344

Owen, G. T. (2014). Qualitative methods in higher education policy analysis: Using interviews and document analysis. The Qualitative Report. 19(26), 1-19. Retrieved from http://nsuworks.nova.edu/tqr/

Pacho, T. O. (2015). Exploring participants’ experiences using a case study. International *Journal of Humanities and Social Science, 5*(4), 44-53. Retrieved from http://www.ijhssnet.com/

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: An insider threat perspective. Decision Support Systems. 92, 47-56. http://dx.doi.org/10.1016/j.dss.2016.09.012

Park, Y. J., Matkin, D. S. T., & Marlowe, J. (2017). Internal control deficiencies and municipal borrowing costs. Public Budgeting & Finance. 37(1), 88–111. https://dx.doi.org/10.1111/pbaf.12120

Parmar, B. (2013). Employee negligence: the most overlooked vulnerability. Computer Fraud & Security, 2013(3), 18-20. http://dx.doi.org /10.1016/S1361-3723(13)70030-7

Petty, R. E., Priester, J. R., & Brinol, P. (2009). Mass media attitude change: Implications of the elaboration likelihood model of persuasion. In J. Bryant & M.B. Oliver (Eds.), Media Effects: Advances in theory and research, (3rd ed.), 125-164, NY: Routledge. Retrieved from https://www.uam.es/otros/persuasion/papers/2009MediaChapterPettyBrinolPriester.pdf

Pezalla, A. E., Pettigrew, J., & Miller-Day, M. (2012). Researching the researcher-as instrument: an exercise in interviewer self-reflexivity. Qualitative Research, 12(2), 165-185. http://dx.doi.org/10.1177/1468794111422107

Pilnick, A., & Swift, J. A. (2011). Qualitative research in nutrition and dietetics: assessing quality. *Journal of Human Nutrition and Dietetics, 24*, 209-214. http://dx.doi.org/10.1111/j.1365-277X.2010.01120.x

Porterfield, M. (2016). Cybersecurity & privacy division. Retrieved from https://nasa.gov/offices/ocio/itsecurity/index.html

Pozzebon, M., Rodriguez, C., & Petrini, M. (2014). Dialogical principles for qualitative inquiry: A nonfoundational path. *International Journal of Qualitative Methods,* (13), 293–317. http://dx.doi.org/10.1177/160940691401300114

Pricewaterhouse Coopers. (2015). Key findings from the 2014 US State of Cybercrime Survey. Retrieved from https://www.pwc.com/us/en/services/consulting/library/us-cybercrime-survey-2014.html

Probst, B. (2016). Both/and: researcher as a participant in qualitative inquiry. *Qualitative Research Journal,* (2)149. https://dx.doi.org/10.1108/QRJ-06-2015-0038

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. Qualitative Research in Accounting & Management. 8, 238-264. http://dx.doi.org/10.1108/11766091111162070

Råheim, M., Magnussen, L., Sekse, R., Lunde, A., Jacobsen, T., & Blystad, A. (2016). Researcher–researched relationship in qualitative research: Shifts in positions and researcher vulnerability. *International Journal of Qualitative Studies on Health & Well-Being, 11* https://dx.doi.org/10.3402/qhw.v11.30996

Rajarajan, G., & Ganesan, L. (2017). A decoy framework to protect the server from wireless network worms. Wireless Personal Communications. 94(4), 1965-1978. http://dx.doi.org/10.1007/s11277-016-3298-5

Rao, A., Carreon, N., Lysecky, R., & Rozenblit, J. (2018). IEEE Software. Probabilistic Threat Detection for Risk Management in Cyber-Physical Medical Systems. (1)38. https://dx.doi.org/10.1109/MS.2017.4541031

Rashad, F. (2014, Nov). Is security awareness training really worth it? Retrieved from Information Week website: http://www.darkreading.com/operations/careers-and people/is-security-awareness-training-really-worth-it/d/d-id/1317573

Reckless, W. (1981). Containment theory - an attempt to formulate a middle-range theory of deviance. National Criminal Justice Reference Service. Retrieved fromhttps://www.ncjrs.gov/App/Publications/abstract.aspx?ID=84235

Resnik, D. B., Miller, A. K., Kwok, R. K., Engel, L. S., & Sandler, D. P. (2015). Ethical issues in environmental health research related to public health emergencies: reflections on the Gulf study. Environmental health perspectives. http://dx.doi.org/10.1289/ehp.1509889

Rezaei, A., Allameh, S. M., & Ansari, R. (2018). Impact of knowledge creation and organizational learning on organizational innovation: an empirical investigation. *International Journal of Business Innovation and Research, 16*(1), 117-133. http://dx.doi.org/10.1504/IJBIR.2018.091087

Ridder, H. (2017). The theoretical contribution to case study research designs. Business research, 10(2), 281-305. http://dx.doi.org /10.1007/s40685-017-0045-z

Roberts, T. (2013). Understanding the research methodology of interpretative phenomenological analysis. *British Journal of Midwifery, 21*, 215-218. Retrieved from http://www.britishjournalofmidwifery.com

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. Qualitative Research in Psychology. 11, 25-41. http://dx.doi.org/10.1080/14780887.2013.801543

Rocha, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture, and awareness. Computers & Security. 5926-44. http://dx.doi.org/10.1016/j.cose.2016.01.004

Rossetto, K. R. (2014). Qualitative research interviews: Assessing the therapeutic value and challenges. *Journal of Social and Personal Relationships, 31*, 482-489. http://dx.doi.org/10.1177/0265407514522892

Safa, N., Sookhak, M., Solms, R., Furnell, S., Ghani, N., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers & Security, 53, 65-78. http://dx.doi:10.1016/j.cose.2015.05.012

SysAdmin, Audit, Network, and Security. (2014). The threat of social engineering and your defense against it. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232

Saunders, M. N. K., & Townsend, K. (2016). Reporting and justifying the number of interview participants in organization and workplace research. *British Journal of Management,* (4), 836. https://dx.doi.org/10.1111/1467-8551.12182

Savola, M. J. (2014). Towards a measurement of security effectiveness enabling factors in software-intensive systems. Lecture Notes on Software Engineering, 2, 104-109. http://dx.doi.org/10.7763/LNSE.2014.V2.104

Scholl, M., Leiner, K., & Fuhrmann, F. (2017). Blindspot: Do you know the effectiveness of your information security awareness-raising program? *Journal of Systemics, Cybernetics, and Informatics, 15*(4) 58-62

Silicon Valley Information Systems Security Association. (2018). Silicon Valley chapter information systems security association. Retrieved from https://sv-issa.org/

Simpson, C. J. (2019). *Unauthorized disclosures of sensitive and classified information: A meta-synthesis of leadership support, security policy, and security education,* *training and awareness within the federal government information security culture* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 13861083).

Sindhuja, P., & Kunnathur, S. (2015). Information security in supply chains: a management control perspective. Information & Computer Security. (5)476. https://dx.doi.org/10.1108/ICS-07-2014-0050

Singh, R., Jiménez, A., & Øland, A. (2017). Voice disguise by mimicry: deriving statistical articulometric evidence to evaluate claimed impersonation. IET Biometrics. 6(4), 282–289. https://dx.doi.org/10.1049/iet-bmt.2016.0126

Sivagnanam, M. (2018). Security measures that help reduce the cost of a data breach. *ISSA Journal, 16*(10), 31–38.

Smith, B., & McGannon, K. R. (2018). Developing rigor in qualitative research: problems and opportunities within sport and exercise psychology. *International Review of Sport and Exercise Psychology,11*(1), 101–121. https://dx.doi.org/10.1080/1750984X.2017.1317357

Smith, J., & Firth, J. (2011). Qualitative data analysis: the framework approach. Nurse Researcher. 18, 52-62. http://dx.doi.org/10.7748/nr2011.01.18.2.52.c8284

Snell, R. (2015). Ten business risk reduction principles. *Journal of Health Care Compliance*, *17*(2), 3.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs a more holistic approach: A literature review. *International Journal of Information Management, 36*, 215–225.

https://dx.doi.org/10.1016/j.ijinfomgt.2015.11.009

Sreevidya, K., & Sumanta, L. (2016). IEEE. *Advanced security analytics*. 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems. 78, 964-975. http://dx.doi.org/10.1016/j.future.2016.11.031

Suen, L., Huang, H., & Lee, H. (2014). A comparison of convenience sampling and purposive sampling. PubMed. http://dx.doi.org/10.6224/JN.61.3.105

Tam, K., Feizollah, A., Anuar, N. B., Salleh, R., & Cavallaro, L. (2017). The evolution of Android malware and android analysis techniques. ACM computing surveys. 49(4), article #76, 1-76. http://dx.doi.org/10.1145/3017427

Tamboukou, M. (2011). Portraits of moments: Visual and textual entanglements in narrative research. Current Narratives. 3, 3-13. Retrieved from http://ro.uow.edu.au/currentnarratives/

Tams, S., Thatcher, J. B., & Craig, K. (2018). How and why trust matters in post-adoptive usage: The mediating roles of internal and external self-efficacy. *Journal of Strategic Information Systems*, 27170-190. http://dx.doi.org/10.1016/j.jsis.2017.07.004

Tavakol, M., & Sandars, J. (2014a). Quantitative and qualitative methods in medical education research: AMEE Guide No 90: Part I. Medical Teacher. 36, 746-756.

Terlizzi, M. A., Meirelles, F. S., & Viegas, M. A. (2017). The behavior of Brazilian bank employees on Facebook and cybersecurity governance. *Journal of Applied Security Research, 12*(2), 224-252. http://dx.doi.org/10.1080/19361610.2017.1277886

Thaler, J., & Helmig, B. (2016). Do codes of conduct and ethical leadership influence public employees attitudes and behaviors? An experimental analysis. Public Management Review. 18(9), 1365-1399. http://dx.doi.org/:10.1080/14719037.2015.1103890

Thomas, D. R. (2017). Feedback from research participants: Are member checks useful in qualitative research? Qualitative Research in Psychology. 14, 23-41. http://dx.doi.org/10.1080/14780887.2016.1219435

Thompson, M. (2017). Unpacking instructional strategies of early childhood teachers: Insights from teachers' perspectives. Educational Research and Reviews. 12(24), 1199–1207. https://files.eric.ed.gov/fulltext/EJ1164626.pdf

U.S. Department of Health & Human Services. (1979). Ethical principles and guidelines for the protection of human subjects of research. Human Subjects Research (45 CFR 46). *The Belmont Report*. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

U.S. Government Accountability Office. (2019). Agencies need to fully establish risk management programs and address challenges. Report to congressional requesters. Retrieved from https://www.gao.gov/assets/710/700503.pdf

U.S. White House. (2018). The cost of malicious cyber activity to the U.S. economy. The Council of Economic Advisers. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Vande Putte, D., & Verhelst, M. (2014). Cybercrime: Can a standard risk analysis help in the challenges facing business continuity managers? *Journal of Business Continuity & Emergency Planning*, *7*, 126-137.

Vass, C., Rigby, D., & Payne, K. (2017). The role of qualitative research methods in discrete choice experiments: A systematic review and survey of authors. Medical Decision Making. 37(3), 298–313. https://dx.doi.org/10.1177/0272989X16683934

Venkatesh, V., Brown, A. S., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. MIS Quarterly. 37, 25-54. Retrieved from http://www.misq.org/

Veronika, M., Klára, T., Krisztina, T., László, N., & Edit, P. (2016). Health behavior of higher education employees – value-transmitting conduct of professionals to their students. Practice and Theory in Systems of Education. 11(3) 162-173

Vilko, J., Ritala, P., & Hallikas, J. (2016). Risk management abilities in multimodal maritime supply chains: Visibility and control perspectives. Accident Analysis and Prevention. http://dx.doi.org/10.1016/j.aap.2016.11.010

Vrij, A., Mann, S., Jundi, S., Hillman, J., & Hope, L. (2014). Detection of concealment in an information-gathering interview. Applied Cognitive Psychology. 28(6), 860–866. http://dx.doi.org/10.1002/acp.3051

Wagstaff, C. R., Hanton, S., & Fletcher, D. (2013). Developing emotion abilities and regulation strategies in a sports organization: An action research intervention.

Psychology of Sport and Exercise. 14, 476-487. http://dx.doi.org/10.1016/j.psychsport.2013.01.006

Walaa, H., Jamal, N., & Bani, S. (2017). A novel technique for securing data communication systems by using cryptography and steganography. Jordanian *Journal of Computers and Information Technology, 3*(2), 110-130. http://dx.doi.org/10.5455/jjcit.71-1494855263

Walker, J. L. (2012). The use of saturation in qualitative research. Canadian Journal of Cardiovascular Nursing. 22(2), 37-46. Retrieved from http://www.cccn.ca

Wang, B., & Li, J. (2014). Study on the model of factor analysis applied in the risk management of electronic commerce enterprise. *International Journal of u-and eService, Science and Technology, 7*(5), 263-270. http://dx.doi.org/10.14257/ijunnesst.2014.7.5.23

Wang, H., Yen, Y., & Tseng, J. (2015). Knowledge sharing in knowledge workers: The roles of social exchange theory and the theory of planned behavior. Innovation-Management Policy & Practice. 17(4), 450-465.

Wara, Y. M., & Singh, D. (2015). A guide to establishing a computer security incident response team (CSIRT) for national research and education network (NREN). *African Journal of Computing & ICT, 8*(2), 1-8. Retrieved from https://pdfs.semanticscholar.org/7358/d4974d246e4ecf2d832a124cb52e69e3c49a.pdf

White, D. E., Oelke, N. D., & Friesen, S. (2012). Management of a large qualitative data set: Establishing trustworthiness of the data. *International Journal of Qualitative*

Methods, 11, 244-258. Retrieved from http://socialiststudies.com/index.php/IJQM/index

Wibral, M. (2015). Identity changes and the efficiency of reputation systems. Experimental Economics. 18(3), 408–431. https://dx.doi.org/10.1007/s10683-014-9410-3

Wierenga, D., Engbers, L., van Empelen, P., Hildebrandt, H. V., & van Mechelen, W. (2012). The design of the real-time formative evaluation of the implementation process of lifestyle interventions at two worksites using a 7-step strategy. BMC Public Health. 12, 1-11. http://dx.doi.org/10.1186/1471-2458-12-619

Wikina, S. B. (2014). What caused the breach? An examination of the use of information technology and health data breaches. Perspectives in health information management, 1 - 16. PMCID: PMC4272442

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies, 120*, 1–13. https://dx.doi.org/10.1016/j.ijhcs.2018.06.004

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing the literature. *European Journal of Information Systems*, *22*, 45-55. http://dx.doi.org/10.1057/ejis.2011.51

Woo, C. W., Cerveny, R. P., & Sanders, G. L. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness, and security compliance. Decision Support Systems. 108, 107-118.

Woods, D., Agrafiotis, I., Nurse, J., & Creese, S. (2017). Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services & Applications*, *8*(1), 1. http://dx.doi.org/10.1186/s13174-017-0059-y

Wu, T., Lee, M., Lin, H., & Wang, C. (2014). Shoulder-surfing-proof graphical password authentication scheme. *International Journal of Information Security,13*(3), 245-254. http://dx.doi.org/10.1007/s10207-013-0216-7

Yang, J. S., Lee, H. J., Park, M. W., & Eom, J. H. (2015). Security threats on national defense ICT based on IoT. Advanced Science and Technology Letters. 97, 94-98. http://dx.doi.org/10.14257/astl.205.97.16

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. Radiologic Technology. 88(2), 225.

Yeboah-Afari, C. (2020). *The role of risk management in business continuity in the information technology sector* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 27744837).

Yin, R. K. (2013). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage.

Yin, R. K. (2017). *Case study research: Design and methods* (6th ed.). Thousand Oaks, CA: Sage.

Younis, A., Kashif, K., & Madjid, M. (2014). An access control model for cloud computing. *Journal of Information Security and Applications.* 1945-1960. http://dx.doi.org/10.1016/j.jisa.2014.04.003

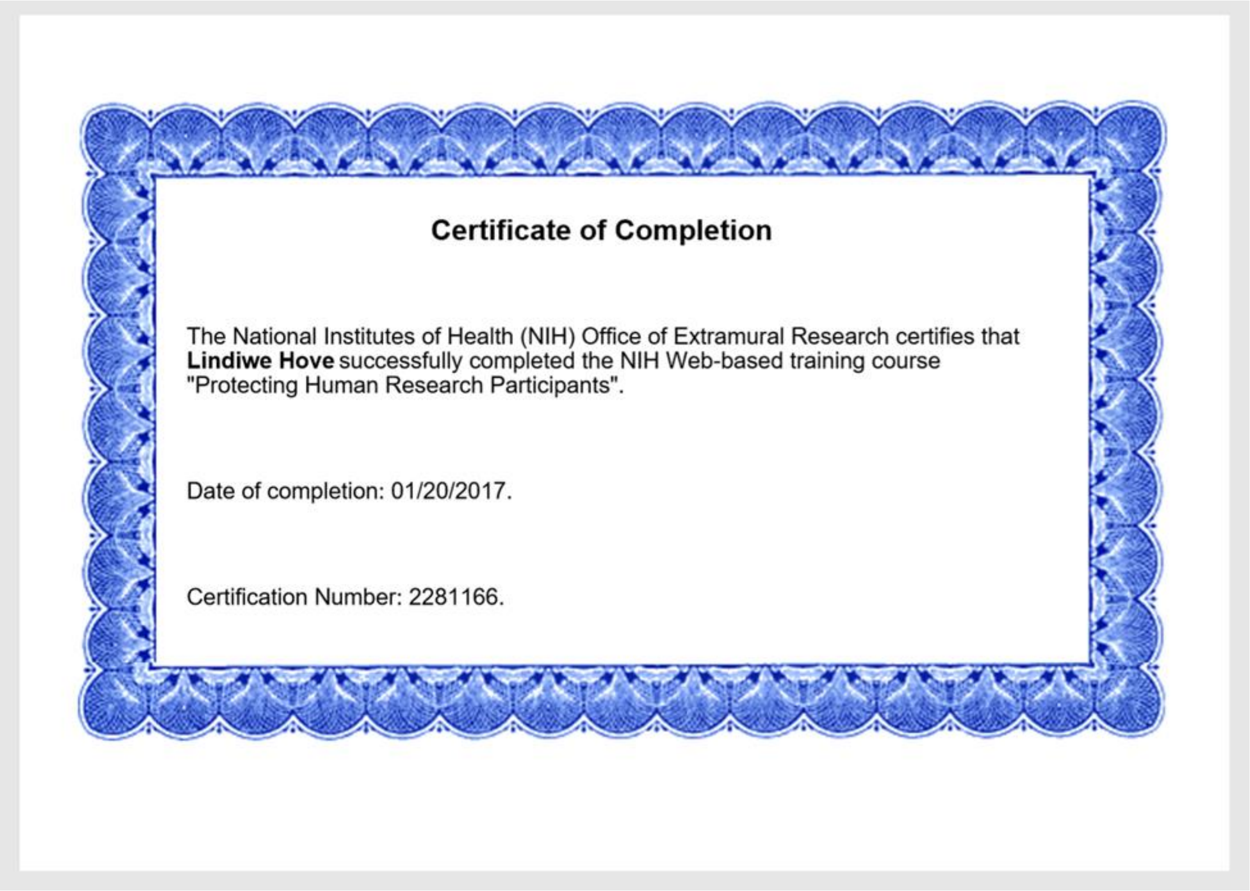
Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal, 27*, 13-15.

http://dx.doi.org/10.4314/mmj.v27i1.4

Zhong, Y., Bhargava, B., Lu, Y., & Angin, P. (2015). A computational dynamic trust model for user authorization. IEEE Transactions on Dependable & Secure Computing. 12(1), 1-15. http://dx.doi.org/10.1109/TDSC.2014.2309126

Zingerle, A. (2014). How to obtain passwords of online scammers by using social engineering methods. *IEEE International Conference on Cyberworlds*. 340-344. http://dx.doi.org/10.1109/CW.2014.54.

Appendix A: Human Subject Research Certificate of Completion



Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Lindiwe Hove** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 01/20/2017.

Certification Number: 2281166.

Appendix B: Interview Protocol and Questions

A. Introduce self to the participant.

B. Verify receipt and respond to the consent form, answer any questions, or concerns of the participant.

C. Get confirmation and acknowledgment that the interview is being recorded.

D. Turn on the recording device.

E. Thank participants for accepting to participate in the study.

F. Start the interview with question #1; follow through to the final question.

G. End interviews and discuss member checking with the participant.

H. Thank the participant for partaking in the study. Confirm the participant has contact information for any follow-up questions and concerns.

I. End protocol.

Interview Questions

1. What does the term social engineering mean to you?
2. How do you assess your information technology security risks?
3. What are some of the challenges when responding to social engineering attacks?
4. What successful strategies do you use for preventing, detecting, and responding to social engineering attack incidents?
5. What employee training strategies do you use for security procedures with Internet devices?

6. What risk management strategies do you use to identify and evaluate social engineering risks?
7. What is your cyber-attack contingency plan?
8. What effective strategies would you recommend to other CISOs to prevent a social engineering attack?
9. What are the management skills needed by technology executives to assist in minimizing social engineering attacks?
10. What are the technical skillsets technology executives need to improve social engineering prevention within corporations?
11. How can technology executives champion best practice data security policies within corporations?
12. What additional information on cybersecurity strategies would you like to provide or expound upon before ending the interview?