2021

Mobile Network Infrastructure Security in Developing Countries – A Kenya Case Study

James M. Omanwa
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

James Omanwa

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. Charlie Shao, Committee Chairperson, Information Technology Faculty
Dr. Steven Case, Committee Member, Information Technology Faculty
Dr. Gary Griffith, University Reviewer, Information Technology Faculty

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

Walden University
2021

Abstract

Mobile Network Infrastructure Security in Developing Countries – A Kenya Case Study

by

James M. Omanwa

MS, Minot State University, 2015

BS, Western Governors University, 2013

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2021

Abstract

The usage of mobile network infrastructure to access internet resources for organizations is getting higher year by year in sub-Saharan Africa. However, there was an increase in malicious attacks on mobile networks and devices accessing mobile network infrastructure, targeting organizations' private information. Grounded in Bandura's social cognitive theory, the purpose of this multiple case study was to explore strategies security managers used to secure mobile network infrastructures from cyberattacks. Participants comprised four security managers in Kenya in two major cities who successfully implemented strategies to mitigate cyberattacks on the mobile network infrastructures. Data were gathered from video conference, face-to-face, semi-structured interviews, and review of organizations' documents comprised of policies and procedures, internal reports, and training procedures. Thematic analysis was used to unveil four themes: security awareness and training, infrastructure management, defense-in-depth, and security governance framework. A key recommendation would be for security managers to craft employee security training and awareness to protect the organizations' data assets. The implications for positive social change include the potential for security managers to mitigate data breaches and protect sensitive customer data from being exposed.

Mobile Network Infrastructure Security in Developing Countries – A Kenya Case Study

by

James M. Omanwa

MS, Minot State University, 2015

BS, Western Governors University, 2013

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2021

Dedication

God Almighty Jah, where have you not taken me and shown me? Every breath I take and every morning I see is a testament to your ever-loving, ever caring, and forever listening father. I could and will never thank you enough for what you have done not only for me but for my family. You took us out of a ghetto, and here I am, achieving a goal that was a distant dream. I take this opportunity to say a simple and humble 'Thank you.'

This dissertation is dedicated to my dearest young brother, the late Dr. Steve Makori Omanwa. He inspired me and showed me the value of teaching others, and by doing that, he nudged me towards academia. You left a hole in my heart that will never be filled, but the legacy you left in your young life equals that of giants; I will forever love you, cherish and hold on to the memories I have of you and remember you for the rest of my life. I will speak of the person you were until my last breath. If there were a way to add a second name to this dissertation, I would add my dear, adorable, caring, and loving wife, Kristen Sexton Omanwa. To say that she has been my support is an understatement. She has been the foundation and rock steady supporter who has worked tirelessly, pushed me, and made sure that I am where I am. I owe everything to you, my love; the English language has yet to invent words that could convey how important and pivotal you have been in helping me achieve this feat.

I am lucky that in my life, I have had women who have been a constant lighthouse in this choppy life. In that breath, I want to dedicate this to my mother, Mrs. Tryphena Moraa Omanwa. My mother has been the grand universe that has given us life and nurtured us; she is our center and the sun that we all revolve around. She labored selling

books door to door, walking hundreds of miles to make sure that we had food on our table, clothes on our back, and we had an education. My mother told us and emphasized that the only ticket out of the ghetto that we grew up in was education; I am forever and will be forever grateful for your love, patience, and wisdom. I also want to dedicate this to my father, Benjamin Mokua Omanwa. Through all, you made sure that we had a good education and taught us the importance of discipline even though we had nothing. I will forever cherish that. I also want to dedicate this to my oldest brother, Kennedy Nyasimi Omanwa. If it were not for you, I would not be here. You took a chance and risked everything to make sure that I got here in this country, and the seer you are, you nudged me to get into the field of computers very early on, and you told me that that is the future. I am here standing on your shoulders. You set a precedent in our family, you trailblazed the path of higher education, and we have all tried to emulate what you have done. Lastly, I want to dedicate this to my children, Caleb, Maxwell, and Amelia. I would never have wished to have better kids than you guys. You guys have been a blessing and absolute Rockstar's. You helped your mom when I need to get my schoolwork done, and you guys were terrific. I am lucky to call myself your dad, and I dedicate this to you three. Someday I hope that you will do better than what your mom and I have achieved.

Acknowledgement

I want to take this opportunity to thank my wife, my rock Kristen, my kids Caleb, Maxwell, and Amelia. I would also want to thank my parents, Benjamin and Tryphena Omanwa, my siblings Kennedy, Kireki, Lillian, Yabesh, my late younger brother Steve for being the best siblings and supporting me in this journey. I want to take a moment and thank a couple of my friends who helped me in different ways to achieve this goal. I want to thank, Jane Njiri, Susan "Suot" Otondi and Steve Giteri for helping me in many ways that I cannot start documenting. I am grateful, Humphrey Muturi, for the motivation and the belief in me even when I sometimes doubted myself. To all, I say 'Shukran' - Thank you, and may the almighty Jah bless you abundantly.

Table of Contents

List of Tables v

List of figures vi

Section 1: Foundation of the Study 1

Background of the Problem 1

Problem Statement 2

Purpose Statement 2

Nature of the Study 3

Research Question 4

Interview Questions 4

Conceptual Framework 5

Assumptions, Limitations, and Delimitations 6

Assumptions 6

Limitations 7

Delimitations 7

Significance of the Study 8

Contribution to IT Practice 8

Implications for Social Change 9

A Review of the Professional and Academic Literature 9

Social Cognitive Theory 11

The Concept of Self-Efficacy in the Social Cognitive Theory 14

Social Cognitive Theory in Different Fields 17

Criticism of Social Cognitive Theory 20
Rival Theories 21
Mobile Network Infrastructure Security 26
Application Security 48
Data Security 51
Mobile Network Infrastructures Security Policies, Laws, and Regulations 57
Mobile Network Infrastructure Security Awareness 60
Mobile Network Infrastructure Security Governance 64
Mobile Network Infrastructure Management 67
Gap in The Literature 72
Transition and Summary 75
Section 2: The Project 77
Purpose Statement 77
Role of the Researcher 78
Participants 80
Research Method and Design 82
Method 83
Research Design 85
Population and Sampling 87
Ethical Research 91
Data Collection 94
Instruments 94

Data Collection Technique 99
Data Organization Techniques 101
Data Analysis Technique 103
Reliability and Validity 106
Reliability 107
Validity 107
Dependability 108
Credibility 109
Transferability 109
Confirmability 110
Transition and Summary 110
Section 3: Application to Professional Practice and Implications for Change 112
Overview of Study 112
Presentation of the Findings 113
Theme 1: Security Awareness and Training 114
Theme 2: Infrastructure Management Tools 118
Theme 4: Security Governance Framework 124
Implications for Social Change 128
Recommendations for Action 131
Recommendations for Further Study 133
Reflections 134
Summary and Study Conclusions 135

References.....137

Appendix: Interview Questions 173

List of Tables

Table 1 *Participants and Organizations* 113

List of figures

Figure 1. Content Analysis Steps..... 96

Section 1: Foundation of the Study

Organizations and private individuals rely more and more on mobile network infrastructure (Thompson et al., 2017). As the mobile network infrastructure and the devices that access the network have become ubiquitous, the rise of breaches of both networks and data on devices has risen (Sen & Borle, 2015). Protection of the mobile network infrastructure and the data traveling on the network is critical. Information technology (IT) managers must cultivate strategies to protect mobile network infrastructures. This issue is even more dire in developing countries due to enterprise and personal data that is not sufficiently protected.

Background of the Problem

According to the research evaluated for this study, network breaches and data theft have constantly been rising globally but more so in developing countries Okuku et al. (2015). Most of these breaches happen due to the lack of useful strategies to protect the mobile network infrastructure. Mobile network infrastructures have become a backbone for organizations. As more and more organizations deploy mobile networks in Sub-Saharan Africa, some constant risks and vulnerabilities accompany the technology.

In this qualitative, multi case study, I reviewed current research on this topic. Okuku et al. conducted a similar study, looking at the exponential rise of mobile network usage and the overall issue of malicious attacks on mobile devices on the network. One of Okuku et al.'s significant discoveries centered on the lack of research done around Sub-Saharan countries and any strategies used to mitigate the attacks on mobile networks and mobile devices. Consequently, my core objective for this research study was to explore

the strategies used by security managers in Kenya to protect mobile network infrastructures from cyberattacks.

Problem Statement

Okuku et al. noted that the usage of mobile network infrastructure to access internet resources for individuals and organizations in Kenya was high. However, there was an 11% increase from 2016 to 2017 of malicious attacks on mobile networks and devices accessing mobile network infrastructure targeting users' private information (Thompson et al., 2017). The general IT problem was that the mobile network infrastructures of business organizations in sub-Saharan Africa are not secured. The specific IT problem was that some security managers lack strategies to protect mobile network infrastructures from cyberattacks.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies used by security managers in Kenya to protect mobile network infrastructures from cyberattacks. The targeted populace for this qualitative multiple case study included security managers from several large and small organizations in Kenya that had implemented strategies to protect mobile network infrastructures from cyberattacks. The potential impact for social change includes the probability of decreasing the theft of important, confidential, or safeguarded individual or enterprise data. Furthermore, the application of cybersecurity strategies may lessen the loss of prospective identifiable data.

Nature of the Study

I used the qualitative method in this study. Qualitative research aims to offer deep insights and study into why individuals engage in distinct actions or conduct (Rosenthal, 2016). The qualitative method was key in determining the strategies that security managers in Kenya use to secure mobile network infrastructure from cyberattacks. Researchers using the quantitative methodology aspire to present a numerical depiction and handling of observations to describe and explain some phenomena that those observations echo (Mccusker & Gunaydin, 2014). Because numerical data were not collected in this study, the quantitative method was not appropriate for this research. Mixed methods research involves combining the quantitative and qualitative research methods in the same inquiry (Watson, 2015). Mixed methods research can be complex and consume a substantial amount of time and energy (Venkatesh et al., 2016). Mixed method research was not appropriate for this research because quantitative data were not collected in this study.

Researchers use the qualitative case study design to understand an intricate social occurrence and investigate and recall a rounded and evocative characteristic of real-life proceedings (Yin, 2013). Since the goal of this study was to comprehend what security managers in Kenya were doing to protect mobile network infrastructure from cyberattacks, a case study was appropriate. Researchers who employ the phenomenological design seek to understand human's lived experiences, mostly relying on the first-person accounts obtained through participant interviews (Charles et al., 2015). I did not seek to understand human's lived experiences, so a phenomenological design

was not suitable for this research. Ethnography aims to understand a group's conceptual world that is seen and experienced from that group's surroundings (Hanus & Wu, 2015). The ethnography method was not suitable for this qualitative research study because its primary goal is to study individuals and interact with the specific audience in their specified surroundings, which did not occur in this study.

Research Question

What strategies do security managers in Kenya use to protect mobile network infrastructures from cyberattacks?

Interview Questions

1. What strategies have you used to protect the mobile network infrastructure from cyberattacks in your organization? Of the strategies that you just mentioned, how were the strategies useful?
2. Of the strategies you used to protect the mobile network infrastructure, what strategies were effective? In your opinion, what made those strategies effective?
3. What other strategies did you deploy to protect the mobile network infrastructure that were not effective?
4. While planning on the strategies to use to protect the mobile network infrastructure, what part did the principle of defense-in-depth play?
5. How do you deploy and incorporate encryption and virtual private network (VPN) in your strategies to mitigate attacks?
6. How do you use wireless security protocols to secure Wi-Fi access points?

7. In your opinion, how do the host-based, anti malware, intrusion detection and prevention systems (IDPSs) and firewalls help mitigate attacks on the mobile network infrastructure?
8. What consideration are application security and data security afforded in the strategies you settled on to protect the mobile network infrastructure from cyberattacks?
9. What part does the use of policies, procedures, and security awareness play in the overall strategies for protecting the mobile network infrastructure from cyberattacks?
10. In your opinion, how do mobile network infrastructure management and governance factor into the overall strategies you deployed to protect the mobile network infrastructure?

Conceptual Framework

The conceptual framework used for this research study was the social cognitive theory. Bandura introduced the social cognitive theory in 1986, and it is a widely accepted theory in behavior, social, industrial, and organizational psychology. The core idea of the social cognitive theory is that environmental impact, personal aspects, and behavior are determined reciprocally (Bandura, 1986). Bandura (1999) stated that one of the significant tenets of social cognitive theory is self-efficacy. Bandura explained that self-efficacy was not what skill an individual possesses, but what that individual does with that skill as well as that the ability to judge and the aptitude to establish and implement a course of action to achieve a selected goal was paramount.

The concept of self-efficacy is not new to the study of information security. In the field of information security, self-efficacy is primarily referred to in the context of security self-efficacy (Mamonov & Benbunan-Fich, 2018). In this research study, I concentrated on the self-efficacy aspect of social cognitive theory.

The social cognitive theory addresses a holistic approach to a person's assessment of a task and that person's ability to do the task confidently (Mamonov & Benbunan-Fich, 2018). Sommestad (2018) observed that social cognitive theory was important in identifying how an individual's perceived utility, belief, and action could help secure mobile network infrastructure. Once individuals have been taught how to secure the mobile network infrastructure and the vital role they hold, their belief in themselves became vital in securing the mobile network infrastructure. The social cognitive theory was used by Sommestad as a framework to understand how an individual could learn, practice, and execute what they had learned by executing what an individual had learned successfully and how that individual's attitude changed. That attitude change could influence the individual's attitude towards how they use the mobile network infrastructure and their adoption of secure habits in general.

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are, in essence, what an individual believes or accepts to be accurate but without tangible proof (Fuchs & Schalljo, 2017). In this research, I assumed that what the participants told me about their organization was accurate. I also assumed participants

would share some insights on what strategies they were deploying to protect their mobile network infrastructure.

Limitations

Levitt et al. (2017) argued that limitations demonstrate what the researcher understands about a topic and that the researcher would not claim generalizability or conclusiveness on what they had learned. According to Garavan et al. (2019), limitations are essential in comprehending the weaknesses of a particular research and are vital in dictating research credibility. Garavan et al. also observed that limitations establish attributes that impact the research's interpretation. In this research, the main limitation was that data collected came from medium to large organizations located in Kenya's capital city of Nairobi and Mombasa, the second-largest city. By concentrating on these two cities, duplication of the research in different areas of the country did not occur. The lacking aspect was due to the absence of organizations with similar mobile network infrastructures in most other medium-sized cities that are rural. Another limitation was the lack of more local, senior IT leaders to interview because most organizations offload technical aspects of cybersecurity to helpdesk, junior-level employees. Another factor was that due to the capital city being a host for multinational companies and nongovernmental organizations, their standards might be higher than those of the local organizations.

Delimitations

Yin (2013) recounted that setting boundaries or delimitations was vital in determining the research scope. A given geographical area and the type of businesses

delaminated the current research study. In this research study, the participants were cybersecurity managers from Kenya who had implemented strategies to combat mobile network infrastructure intrusions.

Significance of the Study

Information about mobile network infrastructure issues in developing countries, and specifically Kenya, was thin and scarce. Although there had been some research conducted on this topic, the researcher did not expressly focus on mobile network infrastructure security or strategies that security managers were deploying to protect their mobile network infrastructure. Given the scarcity of information on this topic, I expected this study to contribute to the information security area and lead to further research studies.

Contribution to IT Practice

Mobile network infrastructures are vital in making sure that information shuttles from one place to another rapidly. Mobile network infrastructures help organizations meet their goals of being efficient, fast, and reliable. Data breaches are costly to the overall impact of the enterprise. Sen and Borle (2015) stated that when it came to data breaches, the average loss of an organization in the United States was approximately $5.9 million. The information gathered in this study can help enterprises worldwide fortify their mobile network infrastructures by providing successful security managers' action plans to mitigate network and data breaches.

Implications for Social Change

The implications for positive social change are that when mobile network infrastructures are secure, then security managers help mitigate data breaches and protect sensitive customer data from being exposed. Data breaches due to insecure mobile network infrastructure also led to data corruption. These breaches directly affect an organization's bottom line and lead to the erosion of trust by its customers (Hinz et al., 2015). Data breaches due to insecure mobile network infrastructure can be multifaceted. They could be in the form of malware that slows down the network or encrypts mobile devices' hardware. They could also be viruses that steal sensitive customer information from databases to be sold on black market sites. The release or selling of customer information data has a reverberating effect. The release or selling of customer data could also lead to identity theft and undermine an individual's security and privacy. Consequently, mitigating data breaches due to insecure mobile network infrastructure would ensure that customers' data has secure parameters keeping hackers or malicious individuals at bay.

A Review of the Professional and Academic Literature

A review of the body of literature on a specific topic has to be well rounded with Baker (2016) arguing that literature reviews should report the current knowledge objectively and provide an overall summary of the preeminent available research about a particular topic. In this literature review, I focus on bringing forth mobile network infrastructure issues due to insufficient security and showing strategies to mitigate mobile

network infrastructure breaches. I also discuss social cognitive theory as the conceptual framework and explain how the theory was pertinent to the research study.

To locate literature for this review, I searched for broader terms related to social cognitive theory and data security on the Google search engine. Some of the results focused primarily on social cognitive theory and network infrastructure. I decided to do more in-depth searches of databases in Walden University's Library for social cognitive theory and network infrastructure security-driven journals. On the network security part, I focused on articles that had a concentration on mobile network infrastructure. I used a variation of keywords for the search, including, but not limited to, *social cognitive theory, network security, data security, mobile networks, mobile network designs, confidentiality, integrity, availability, mobile network infrastructure policies, mobile network infrastructure implementations, mobile network management, authentication and authorization,* and *mobile network security laws and regulations*.

All the pertinent information regarding my literature review came from Walden University library databases and various dissertations (i.e., from ProQuest Central, ScienceDirect, Academic Search Complete, and Google Scholar). I also used Ulrich's Periodical Directory to verify that the journals I was sourcing were peer reviewed. This literature review consists of 237 articles, of which 229 (95%) are peer reviewed and 222 (93%) were published within 5 years of expected chief academic officer approval.

The information reflected in this literature review provided the scholarly underpinnings for this research study. The information also helped me examine the existing body of knowledge regarding strategies used for securing mobile network

infrastructure by information security managers. This literature review has three major components: the conceptual theory, the mobile network infrastructure, and the strategies used. Furthermore, the strategies used category includes the following subcategories: (a) mobile network infrastructure awareness; (b) mobile network security governance; (c) mobile network security laws and regulations; (d) mobile network authentication and authorization; (f) confidentiality, integrity and availability; (g) data security; (h) firewalls, encryption, antiviruses, and IDPSs; and (i) mobile network management.

Social Cognitive Theory

The underpinnings of Bandura's (1986) theory emanate from the triplex model comprising three influential factors: the person, the environment, and the behavior. These three aspects form the core components of social cognitive theory. These foundational aspects have a reciprocal impact on each other. By that, they also impact an individual's modeling, self-efficacy, observational knowledge, self-control, and foresight (Bandura, 1986). Weger and Wagemann (2015) argued that in qualitative inquiry, in general, a person refers to a human who could give a perspective to the research study and could give an introspective approach to the strengths or limitations of a subject. On the other hand, Sörqvist (2016) argued that the environment in qualitative research was the basic structure of an individual's daily life. An environment in a broader sense could also be the holistic relationship between built and natural characteristics of the world around us as individuals. Lastly, Aunger and Curtis (2016) observed that behavior was a key component of how individuals act or carry themselves around or towards other people. Additionally, Rubenstein et al. (2018) noted that the likelihood of rewarding a behavior

could influence the behavior itself. The act of understanding may emerge by applying such methods and mechanisms that are emblematic.

Each individual learns differently, and one of the ways an individual may learn is by modeling what someone else was doing. Modeling focuses on the individual as they learn from another person, and a person is one of the essential columns of social cognitive theory (Bandura, 1986). The social cognitive theory is centered on modeling; through modeling actions, there are probabilities that a person could learn the pragmatism and relevance of a behavior (Bandura, 1986). In this way, an individual can learn a behavior without acting or performing the behavior. Beauchamp et al. (2019) observed that an individual could learn behavior by observing someone else do or undertake the behavior. On the other hand, Lin and Chang (2018) indicated that an individual might learn through different symbolic learning; this can be audiovisual, viewing a video, and reading materials (e.g., books, brochures, etc.). Amongst the acts advanced by Bandura (1986) are observational learning, reticence and disinhibition, and response simplification. In this study, reticence and disinhibition were not applicable; instead, I concentrated on response simplification and observational learning. For observational learning to cement, a person must be determined to learn observationally.

Motivation is a crucial characteristic of modeling and observational learning (Lin and Chang, 2018). Motivation can emanate from the environment that an individual is in, and the environment is also a key component of social cognitive theory. Bandura (1998) stated that a person would be disposed to preserve and produce actions that they perceive to be important. Individuals also tend to hold onto deeds that contribute to productive

outcomes and, consequently, avoid actions that may lead to a negative consequence. Ozyilmaz et al. (2017) noted that observational learning tends to happen when an individual witnesses another individual display behavior that would not have naturally transpired. One vital facet of observational learning is how to create and sustain new conduct. Ozyilmaz et al. indicated that observational learning encompasses four distinct processes: attentiveness, preservation, practice, and production. Through the attention process, an individual is aware of the learning goal, and the retention process involves the individual being able to absorb what they are learning. The rehearsal process allows the individual to put what they learned into practice, and lastly, the production process involves the individual being able to perform what they learned regularly.

Furthermore, Bandura (1986, 1998) added that an individual's awareness of the consequences of their conduct could help change the individual's behavior. Beauchamp et al. (2019) argued that penalties could convey to an individual what needed to change to attain an outcome and the appropriateness of that conduct. Creative ideas can be a framework that conjures suitable responses and standards that improve an individual's performance (Rubenstein et al., 2018). Rubenstein et al. also found that a person's learning accomplishment was a topic of observational learning. The person who was learning by explicit example determined perceptions of their actions built on penalties. A person must have jurisdiction over their tenets and believe in their capabilities to execute or realize new conduct.

The Concept of Self-Efficacy in the Social Cognitive Theory

Bandura (1998) argued that self-efficacy was a central concept in social cognitive theory because an individual's self-assessment was a key determinant of their behavior. An individual's behavior has the power to influence the amount of effort they would input to overcome an obstacle. Honicke and Broadbent (2016) referred to self-efficacy as a person's ability to judge their capabilities to self-organize and be competent to execute a plan required to achieve the desired performance. Additionally, Boateng et al. (2016) stated that the main argument of social cognitive theory was that a person's behavioral purpose was a primary role of behavior and some degree of influence was taken from perceptive personal behavior and that person's surrounding factors. Therefore, self-efficacy is a vital pillar of the theory. Individuals who have elevated self-efficacy are inclined to demonstrate specific presentations and continue to be active in working towards a specific goal. Self-efficacy is an individual's confidence in themself and having strong credence in their abilities to attain a goal.

In the social cognitive theory, Bandura (1986) argued that a person's beliefs in their ability to master or perform an action at a level were significant. Furthermore, Panadero et al. (2017) added that self-efficacy contrasts from knowing what a person could do, but instead, self-efficacy compares with one's self-proficiency to get something completed. On the other hand, Boateng et al. (2016) noticed that self-efficacy was essential to agency or being a self-starter to galvanize people to alter their lives. Moreover, self-efficacy is juxtaposed with self-concept, which is the totality of an individual's view of themself formed by cooperating with their ecosystem, decoding this

interaction, and getting a response from others. Self-efficacy also varies from self-esteem, which correlates to assessing a person's self-worth (Panadero et al., 2017). Bandura (1986) defined procedures such as taking an action and executing what an individual had learned, and that was incorporated as self-management in an individuals' behavior making and self-evaluation concerning a specified objective.

As argued by Elst et al. (2014), the cognizance of efficacy encompasses the cognition of the efficacy of a recommended response and the efficacy of a person acting on a response. When recognizing that both action and response from the person acting was being taken to consideration, the latter was known as self-efficacy. Self-efficacy is the magnitude to which individuals have confidence in their innate ability to enact a recommended action or response (Huang, 2016). Self-efficacy is the credence in organizing and accomplishing a mission via action progression (Bandura, 1986). Self-efficacy comprises a person's trust in their capability to motivate themselves, marshal up cognitive resources, and chart what path of action is desirable to implement a specified task or event (Bandura, 1998). Siciliano (2016) argued that self-efficacy channels down to an individual's convictions and abilities to mobilize themself, have a course of action, and be driven to get the task at hand done successfully.

Self-efficacy has been used and deployed in different fields. Panadero et al. (2017) deployed self-efficacy to analyze the impact of academic performance in tertiary education. On the other hand, Shoji et al. (2015) used self-efficacy to unpack the strong point of the connection between self-efficacy and job burnout on teachers and health care field. Self-efficacy has also been used in the health care realm. Sheeran et al. (2016) used

self-efficacy to decide if altering attitudes or ideals helps patients' purposes and behavioral changes.

In the IT field specifically, self-efficacy has been deployed in different ways. IT uses self-efficacy through the notion of computer self-efficacy. A core concept of computer self-efficacy encompasses an individual's judgment of their capability to utilize a computer in different situations when the need arises (Aesaert et al., 2017). Computer self-efficacy was derived from the general concept of self-efficacy and was introduced by Davis et al. (1989) and Gist et al. (1989).

Computer self-efficacy plays a vital role in information security. Hina and Dominic (2018) stated that information security encompasses three essential traits: availability, integrity, and confidentiality. Rhee et al. (2009) argued that to espouse the general definition of computer self-efficacy, a person had to align and be precise on an information security framework. Self-efficacy in information security expounds on a person's confidence in their capability to safeguard data and mobile network infrastructure from individuals who are not authorized and protect the data from loss, destruction, modification, and unavailability (Rhee et al., 2009). Workman et al. (2008) noted that self-efficacy embodies an individual's set of abilities in practicing information security and taking measures to protect data.

Ng et al. (2009) noted that many researchers had observed self-efficacy in computer security as a key precursor to secure user behavior. Furthermore, Huang (2016) added that information security self-efficacy could be a straight path that could direct an end-user behavioral objective in cybersecurity compliance. Moreover, Ng et al. argued

that self-efficacy in information security could improve security behavior and act as a critical determinant of threat mitigation motivation in an individual, finding the curiosity for self-efficacy in information security as a precursor of information security compliance materialized more than any precursor variable. Sommestad (2018) stated that computer security self-efficacy was researched more than seven times in different studies, while different other variables accounted for not more than one study.

Social Cognitive Theory in Different Fields

Social cognitive theory has been used and deployed in different fields as a foundational theory. Although the theory has been used more in psychology, there are quite a few cases out there that the theory has helped define in fields of study unrelated to psychology. Schoenfeld et al. (2017) used social cognitive theory to explore professors' correlation in academia and their accounting students. Schoenfeld et al. used the social cognitive theory to map out how students' career interests and goals connected to their self-efficacy belief and the expected outcome.

To explore the correlation between professors and their accounting students' ability to be certified public accountant. Schoenfeld et al. (2017) began with a survey instrument consisting of 16 questions; these questions needed the individual to respond on a 5-point scale. The review was on 228 undergraduate students who were taking a needed accounting class for their major. Out of the 228 students, 15 students responded with incomplete surveys resulting in a sample of 218. Schoenfeld et al. worked with a dependent variable based on the undergraduate's aptitude to become a certified public accountant. Two independent variables estimated the outcome and respondent's self-

efficacy, measured by a single question assessing the person's self-assurance in their capacity to become a certified public accountant. By deploying social cognitive theory, the researchers found that the professor's correlation and the ability to motivate their students played a part. However, the student's own motivation to be a certified public accountant played a key role too.

On the other hand, the social cognitive theory was a key instrument used for a foundational study to understand the correlation between the high-risk age bracket of college-aged females exposed to the risk of human papillomavirus infection (HPV). Catalano et al. (2016) utilized social cognitive theory to envisage unvaccinated university women between the ages of 18-26 – who aim to obtain the HPV vaccine in the next 12 months. The researchers utilized social cognitive theory's framework to help bring forth what their research aimed to show.

To show a holistic picture of research, the importance of capturing the right data was essential. Catalano et al. (2016) utilized interview questions to amass data from the respondents. A total of 197 unvaccinated university-age women between the ages of 18 and 26 took an online questionnaire. The study was further broken down to expectations, knowledge of the vaccine, self-efficacy to obtain the HPV vaccine, and self-efficacy in dismantling hurdles to get the vaccination (Catalano et al., 2016). By using social cognitive theory, the researchers were able to conclude that sexuality educators were instrumental. The researchers found that by raising self-control and raising a situational perception, there were chances of increasing HPV vaccination on university-age women.

The social cognitive theory was a crucial component in the study of post traumatic stress adoption in a holistic view of mass violence. Smith et al. (2017) used the theory in the framework of mass violence. The utilization of general self-efficacy like pre-event defensive influences and social backing could reduce post-traumatic stress syndrome. Smith et al. used social cognitive theory and self-efficacy as a model to study how boosting post event self-efficacy could be instrumental to individuals. The qualified hypothesis put forward by Smith et al. stated that they predicted that post-event social support barriers do interrupt health promotion by indirectly affecting pre-event protective factors. The study encompassed 70 university students enrolled during mass violence events, and they completed a twelve-month survey before an event and six months after an event. As a framework, social cognitive theory helped the study results reinforce the premise put forward by the researchers.

Some researchers have used social cognitive theory in the information technology field to explain various issues and map out solutions. Kim and Park (2017) used social cognitive theory to show factors influencing one's actions in utilizing e-learning in emerging market countries. Kim and Park concluded that performance and computer self-efficacy were essential factors shaping behavior intent in utilizing e-learning. As long as there had been those who view social cognitive theory as instrumental in helping craft research, some have had a different view of the theory itself. Some researchers have criticized the theory as not wholly enough to help with a research study.

Criticism of Social Cognitive Theory

Social cognitive theory, as a cornerstone theory, could be an essential tool in a research environment. Social cognitive theory plays a vital role in emphasizing an active, interactive course among an individual's environment, behavior, and personal factors regarding functioning (Bandura, 1986). As social cognitive theory has continued to be used and deployed in many fields, some researchers did observe some weaknesses in the theory itself. Burney (2008) looked at social cognitive theory as a foundational theory, but it lacked depth in other areas. Burney believed that motivation was essential from a person's self-efficacy awareness and a conducive environment. If the environment lacked for an individual to learn from, then the theory's whole structure could come into question (Burney, 2008). Other researchers like Burney and Rhee et al. (2009) have deployed social cognitive theory and, in some cases, found the theory as inadequate.

The inadequacy and limitations of social cognitive theory could stem from different issues. Rhee et al. (2009) observed that social cognitive theory focused on the situation and environment overshadows other essential traits. An individual's emotions and personality could be critical in learning capability (Rhee et al., 2009). While situations and environments were critical, traits also play a major role in one's learning ability. On the other hand, social cognitive theory does seem to emphasize the overall cognitive aspect. Ng and Lucianetti (2016) pointed out that biological and hormonal processes could be instrumental in how individuals make decisions. Decision-making could be affected regardless of past experiences and cognition (Ng & Lucianetti, 2016).

In this aspect, the social cognitive theory does not consider the importance of biological influences on how individuals decide what to do.

Some researchers have mulled over the issue of self-efficacy regarding social cognitive theory as a whole. Rana and Dwivedi (2015) argued that social cognitive theory could have some neglected areas. There was a lack of involvement of maturation over the lifespan of an individual in theory. Rana and Dwivedi observed a lingering question if individuals retain more as they mature in general.

On the other hand, the social cognitive theory does not focus more on motivation and conflict and its effect. Rhee et al. (2009) observed that the lack of how individuals learn and act on what they had learned was affected by conflict, and motivation was essential. Some researchers who have used social cognitive theory believed that the theory was not well equipped to study deeper research aspects. Some researchers thought that the theory could impact how an individual learned and retain what they learned.

Rival Theories

Activity theory

Activity theory was one of the theories that looked similar but are structurally different from social cognitive theory. Activity theory is a basis that holistically defines a set of structured interactions in an individual (Holen et al., 2017). At its core, activity theory offers a window through which data could be interpreted (Holen et al., 2017). Holen et al. also argued that activity theory seen through the Vygotsky model acts as a representation of an interaction between a subject, an object, and a tool. The subject was

the individual; the object was the goal of that individual, and the tool was the artifact that facilitates the action of realizing the eventual goal (Carvalho et al., 2015).

The simple basis of activity theory was the activity itself. Kaptelinin and Nardi (2017) argued that there was no meaning to activity theory if there was no context. The context could include or be influenced partly by history, personal motivation, artifacts, or the environment (Holen et al., 2017). In comparison to social cognitive theory, the emphasis was engrossed in helping the individual to be able to learn and execute goals independently. Activity theory could be applied to illuminate the basis of information quest and information behavior. Carvalho et al. (2015) argued that activity theory was increasingly being used and applied in the information systems security realm. While both theories help facilitate how individuals learned from their peers and their environment on information security matters, they differed in their approach.

Activity theory could be a capable instrument for analysis when used to measure individuals' interactions and their goals from those interactions. Gedera (2016) stated that the theory could explain the complex process of human perception's growth: how individuals make meaning of their environment through interactions with other people and artifacts. Activity theory could be functional in information technology security (Korpela et al., 2007). Such is the case of an individual's perception and reaction to information security and how individuals could learn to protect the mobile network infrastructure. As Gedera focused on how an individual's perception propels an individual using activity theory to learn, Boateng et al. (2016) observed that an

individual's behavior and intention spurred in social cognitive theory the motivation to learn and self-execute a goal.

As a researcher, the use of activity theory could be beneficial. Kaptelinin and Nardi (2017) found that activity theory could be instrumental in learning in a social setting, which was important in an information security environment. Although activity theory and social cognitive theory could seem similar in social and environmental learning, I observed that social cognitive theory was more foundational than activity theory. The social cognitive theory encompasses observational learning, behavioral capability, reinforcements, expectations, and, most of all, self-efficacy. These factors make social cognitive theory a more robust and versatile theory for me to use. I used social cognitive theory to study the challenges that information security managers face as they try to secure mobile network infrastructures.

On the other hand, the social cognitive theory addresses the inclusive process used to address how an individual's motivation and environment could be impactful. Ng et al. (2009) believed that social cognitive theory would be instrumental in shedding light on how information security managers could inspire employees to be proactive. However, one of the essential tasks for security managers was getting employees to adhere to their training. Researchers have deployed the use of social cognitive theory in the field of computer and network security. Huang (2016) observed that self-efficacy, a tenet of social cognitive theory, merges an individual's belief in oneself and the organization's objective of securing the network infrastructure. Huang argued that individuals' ability to learn and act on what they learned was essential. The securing of

an organization's network infrastructure depended on the employees and users. Information security managers must teach employees so that the employees could learn and act on what they learned. By practicing what they learned, the chances of mitigating attacks on the mobile network infrastructure would increase.

Theory of Planned Behavior

A competing theory as a comparison was the theory of planned behavior. Lapkin et al. (2015) stated that the theory's foundation was in the proposition of a model on how human action was engaged. On the other hand, Ajzen (2014) argued that the theory had a depth of range in different behavioral intentions and behaviors.

However, planned behavior theory was said to have a set of core constructs to the theory itself. There are some similarities and differences between both theories. A core belief of the theory of planned behavior points out that it could lead to behavioral constructs and guide an individual to perform a specific behavior. Mullan et al. (2015) argued that the theory had the intention and focused on the formulation of a plan to do or behave in a certain way; this included instructional material and technology in a job setting. These were some similarities that mirror social cognitive theory. However, the difference between the two focused on how the individual executed what they had learned, further retention, and practice (Elst et al., 2014). Many foundational works of literature pointed out that the proposal put forth by the theory of planned behavior was reliable. Lapkin et al. (2015) stated that hundreds of researchers had deployed the theory of planned behavior, proving its efficacy.

For an individual to be able to not only learn but also carry out what they had learned, there had to be motivation first and foremost. Davis et al. (1989) stated that planned behavior theory was a good analytical tool to show how individual behavior control and subjective norm could be critical contributing variables to behavior intentions capped with attitude. Researchers have used the theory in the realm of computer and network security environments. The theory could be applied to point out the factors of behavioral control, subjective norms, and how individuals' attitudes towards information security could be shaped (Ng & Lucianetti, 2016). On the other hand, Lebek et al. (2014) also used planned behavior theory. However, Lebek et al. substituted alleged behavioral control with self-efficacy, which the researchers saw as fundamentally equivalent.

The theory of planned behavior has been used by researchers as a foundational theory when it comes to information security. Lebek et al. (2014) argued that the theory of planned behavior might explain how individuals conform to information security policies due to security attitudes. In time, the attitude shaped the behavior, and thus one of the key differences between the theory of planned behavior and social cognitive theory. Since the theory of planned behavior emphasized attitude, the social cognitive theory focused on the individual's self-belief to execute a security objective. Herath and Rao (2009) also observed that attitude play's a big part in showing the association with an individual's policy compliance intentions. Lebek et al. further argued that attitude was an outcome of self-efficacy and behavior principles. The theory of planned behavior could be employed to show how an individual's attitude towards information security might be shaped by what and how they view security, which was important.

Ultimately, social cognitive theory, activity theory, and theory of planned behavior are theories that are in some ways similar but also different. While social cognitive theory dealt with the individual's holistic approach to carrying out a task, activity theory focused on context. Consequently, the theory of planned behavior core construct was similar to social cognitive theory, but the deviation between the two theories was vital to remember. The theory of planned behavior focused on the plan and how to carry out the plan, while social cognitive theory concentrates on individuals' belief in themselves. Social cognitive theory's framework could help some qualitative researchers thoroughly discuss their research studies. The next section of this literature review looked deeper into the mobile network infrastructure security entails strategies and implementations that would be important in securing the mobile network infrastructure.

Mobile Network Infrastructure Security

To learn how information security managers could tackle issues that affect mobile network infrastructure, they have to accommodate all perspectives. These perspectives could be broad, and since the mobile network infrastructure is an ecosystem, there are parts of that form the core network. The core aspects of the mobile network infrastructure included the network, applications, and data. Tong and Yan (2017) observed that the network, applications, and data form the foundation of communication in some organizations. As data is becoming a keystone for organizations, securing the mobile network infrastructure and applications that facilitate the data to move from one place to

another is essential. Security managers have to start securing the mobile network from the perspective of the network first.

Security managers' mission is to secure the network itself. The mobile network infrastructure plays a major part in some organizations. Kos et al. (2019) observed that some organizations leveraged the mobile network infrastructure's efficiency to their advantage. The advantage of the mobile network infrastructure lay in the ease of use of devices by users from different locations without being tethered to a central location. Carter et al. (2018) argued that the mobile network infrastructure's ease and efficiency emanated from cabling's absences that would have confined a user to a location. By accessing resources from different locations, the mobile network infrastructure was vital, but it also formed the core of some organizations' communications. Therefore, the need to protect the mobile network infrastructure had to be paramount. The security of the mobile network infrastructure from a defense-in-depth perspective was essential.

As organizations become more reliant on network infrastructures, investing in the mobile network infrastructure's security was paramount. Sarika et al. (2016) observed that network security was foundational, and without a robust security plan, a network could be vulnerable to cyberattacks. Mobile network infrastructure security was essential, and different aspects of securing the network are vital. One of the key aspects of securing the mobile network infrastructure was using a defense-in-depth as an overall security principal.

A defense-in-depth security principal uses layered security strategies for countermeasures to secure a network infrastructure (Jander et al., 2018). Defense-in-

depth uses the fundamental principle that the defeat of multiple barriers is more challenging than the defeat of a single barrier. Jander et al. noted that using a multi-layered approach with deliberate redundancies could enlarge the security of a network, and by doing that, address the various attack vectors that hackers might use. Additionally, using a multi-layered security approach could minimize the probability that an intrusion on the network succeeded. Al-Safwani et al. (2018) also observed that a well-designed defense-in-depth strategy could help systems administrators and security managers identify any attempt to compromise the network infrastructure resources. If an individual with malicious intent were to gain access to the network infrastructure, a multi-layered defense approach would minimize the network's adverse impact (Al-Safwani et al., 2018). By minimizing the network's adverse impact, the security personnel and systems administrators could deploy and update countermeasures to mitigate future recurrence.

To secure the mobile network infrastructure, security managers must incorporate a robust strategy to their mobile network defense. A multi layered security approach could be an important strategy in securing the mobile network infrastructure. Sarika et al. (2016) argued that security managers could deploy a defense-in-depth method to secure the mobile network infrastructure. By deploying defense-in-depth as the principal, the strategies that make defense-in-depth include encryption, firewalls, IDPSs, Anti-malware, authentication, and authorization help organizations mitigate attacks of the mobile network infrastructure. As organizational needs vary, one of the key elements of a defense-in-depth that organizations need was encryption.

Encryption

The fundamental process of changing data into a different form or code to have it obscured by individuals who do not have the right access to it is called encryption (Stallings, 2016). Data that is encrypted is called ciphertext (Stallings, 2016). Encryption has become a staple in securing data. Etaiwi and Hraiz (2018) added that some organizations use encryption as one method of securing data. There are different types of encryption; Rawal (2018) revealed that the two main types of encryption are public-key encryption or asymmetrical encryption and symmetric encryption.

The two types of encryptions work differently, but they fundamentally had the same purpose. Public key encryption or asymmetrical encryption permits each to have two keys – a private and public key (Li et al., 2018). The keys are connected, and in actuality, they are large numbers that had mathematical properties. Li et al. indicated that when individuals used their public key to encode a message, the other individual had to use their private key to decode the message. On the other hand, symmetrical encryption comprised one key to encrypt and decrypt the data (Zhou & Yang, 2017). Symmetric was faster and secure in many aspects when used locally but does not work well when going from network to network; this was because it had to be sent together with the key across the networks (Zhou & Yang, 2017). Data encryption has become a staple in most organizations, and most organizations are deploying encryption to safeguard data.

The core aspect of data encryption was to protect the data's' confidentiality. As organizations send and receive confidential data, ensuring their data was not tampered with or stolen was paramount (Ahmed & El-Henawy, 2017). Ahmed and El-Henawy also

stated that the algorithms give confidentiality and security initiative capabilities that included authenticating, integrity, and non-repudiation. Using authentication, one could verify the origin of the data; integrity maintains that the data's content did not go through any modification, and non-repudiation warrants that the sender could deny sending the data (Etaiwi & Hraiz, 2018). Organizations have to secure data whether it is at rest or in transmission, and thus, encryption plays a significant role.

Data continues to be a vital part of organizations. Encryption offers the solution of protecting data used by applications on devices, shared via email, and the data itself (Etaiwi & Hraiz, 2018). In many aspects, encryption had a functionality layer that adds control for applications (Zhou & Yang, 2017). Organizations are facing challenges on how to protect and prevent data loss. As employees use external devices, mobile, and web applications daily, sensitive data could be visible to malicious software and hackers (Ahmed & El-Henawy, 2017). The need to have a method to secure data was important as organizational data assets grow. The use of encryption on applications was a good foundation from a mobile network infrastructure perspective.

Organizations' data assets are important, and it is paramount, whenever data was at rest on the mobile network, the data had to be stored and protected. Potey et al. (2016) noted that data-at-rest encryption could be pivotal as the last line of defense of data at rest in an organization's mobile network infrastructure. Potey et al. further stated that data-at-rest encryption added a security layer and access control to the organization's sensitive data when stored. Some of the organizations' most sensitive data were in databases, applications, web servers, and file servers. Data-at-rest encryption could serve as last

resort security for the data stored in databases, applications, and file servers (Potey et al., 2016).

Furthermore, data-in-motion is data as it moves from one place to another (Stallings, 2016). Unprotected data in transit could be vulnerable to attacks (Potey et al., 2016). The need to have encryption as a protection for data in transit was important. Moreover, Rawal (2018) noted that encryption was an effective way to safeguard data in transit. As data either traverse or rest, encryption could be a key strategy that information security managers deployed. Nevertheless, encryption does have challenges.

Encryption, like other deterrence strategies, also could be attacked. One of the most common encryption attacks was specialized software to brute force the encryption keys (Yang et al., 2019). Yang et al. revealed that a brute force attack tried a random set of keys until the right one was exposed. In this aspect, the key's length determined the probable number of keys that a hacker could try. Yang et al. also stated that it was crucial to remember that the encryption strength was relatively proportional to the key size. However, as the key size increased, the amount of computing resources needed to process the encryption also increased (Etaiwi & Hraiz, 2018). A side-channel attack could also be applied to exploit encryption. The side-channel attack looks for weakness in the encryption itself rather than the encryption keys (Potey et al., 2016). The success of these types of attacks on encryption could be devastating. Side-channel attacks tended to be disruptive to a targeted host if there were errors in the system design or, in some cases, how the encryption was executed (Potey et al., 2016).

Encryption could be deployed in different ways depending on the network. Security managers had to be able to deploy encryption in different ways to protect data. Stallings (2016) noted that for a mobile network, encryption was utilized on mobile devices by the use of hypertext transfer protocol secure (HTTPS), virtual private network, and also the utilization of secure wireless protocols. One of the key elements of encryption ensured that if someone did not have access to the data, they could not see what was on the data. Encrypting a mobile device protected the device's drive with a password or alphanumeric pin (Ahmed & El-Henawy, 2017). The only way anyone could access that mobile device was by having an encryption key, meaning that the data was safe if, by any chance, that the device was stolen or lost. Ahmed and El-Henawy noted that having a mobile device encrypted achieves the core tenet of security, but disadvantages may arise. One of the disadvantages was that the mobile devices might have a slight reduction in performance due to decrypting the drive before use; also, the encryption was one way; once the drive was encrypted, you could undo the encryption (Zhou & Yang, 2017). Also, mobile devices used for access to resources via the internet were essential. Stallings (2016) argued that due to the use of the internet to access resources, the use of HTTPS had to be essential to protect data between the mobile devices and the mobile network infrastructure. HTTPS could help establish an encrypted tunnel between the mobile devices browser and the server by using a secure socket layer or by utilizing transport layer security, which is a newer version of SSL (Potey et al., 2016). HTTPS use ensured that the data sent back and forth from the mobile devices to the mobile network infrastructure was secure from any prying eyes.

On the other hand, there had to be a secure channel for communication between mobile devices and mobile network infrastructure. A virtual private network fills in the gap for that secure channel (Yang et al., 2019). VPN form a secure tunnel that allows devices to connect to the organization's mobile network infrastructure securely. Potey et al. (2016) observed that VPN utilization could help users have mobile access to the organization's network through persistent encrypted tunnels and secure data as the data transverses back and forth. VPN could be instrumental in how devices in the mobile network infrastructure communicate back and forth securely. Also, the backbone of communication on the mobile network infrastructure is the wireless access points. Wireless access points facilitate data communication via radio waves from one location to another (Mahmud et al., 2019). The security of these radio waves was important. Mahmud et al. noted that wireless security protocols are fundamental in securing communication between mobile access points. The most commonly deployed wireless security protocol was the Wi-Fi protected access to Version 2 (WPA2). Asimi et al. (2018) observed that WPA2 was more versatile due to the American encryption standard as part of the security standard to protect transmitted data. Asimi et al. noted that WPA2 pre share an encryption key combined with the device's identification to transmit encrypted data; they used a pairwise transient key to enable the encryption and decryption of data packets. The combination of WPA2 and AES makes it hard for anyone with malicious intent to snoop through the radio waves, capture and read the data packets as they are traversing back and forth on mobile network infrastructure.

The utilization of encryption to secure data was paramount. Security managers have the responsibility of making sure that employees know the importance of encryption. By teaching employees how to use and deploy encryption, security managers empowered those employees, therefore fulfilling a social cognitive theory tenet of self-efficacy. Therefore, the importance of security managers being able to teach and mentor employees was key to self-efficacy. On the other hand, organizations that invest in encryption also needed to couple it with another strategy for it to be formidable. Information security managers could be better equipped by adding encryption with another form of data security, like a firewall.

Firewalls

Firewalls play an essential role in protecting data from unauthorized access. Khoumsi et al. (2018) stated that firewalls act as a barrier and shield that protected devices and data from external threats. Organizations are finding that firewalls could be an essential aspect of protecting devices and sensitive data. Khoumsi et al. further stated that, with the increased use of sophisticated software by hackers to probe and attack networks, well-configured firewalls could be an added security layer. Some organizations deployed firewalls as one of the first lines of a defense-in-depth strategy for the mobile network infrastructure.

Firewalls work by inspecting all the traffic coming in and out of the network (Salah et al., 2017). Data that passes in and out of organizations could be enormous at any given time, and in that data, malicious data might sneak in too. Khoumsi et al. (2018) revealed that firewalls not only act as barriers but also isolate the network. By isolating

the organization's network from external networks, firewalls inspect any data packet coming in and out to ensure it was not malicious (Salah et al., 2017). Furthermore, firewalls could help the internal segmentation of a network. Ghanbari et al. (2015) added that firewalls could be applied to isolate and protect internal segments of a network such as data centers from the other networks in an organization. Firewalls use different methods to identify if the traffic coming in should be allowed or dropped. Tran and Ahn (2017) further wrote that firewalls could deploy different types of signatures and conditions set to allow or deny traffic. Firewalls could be a useful tool for an information security manager when utilized to protect the network infrastructure.

As technology advances, firewalls are also becoming more sophisticated to deal with newer strains of malicious data (Ghanbari et al., 2015). There are several types of firewalls that an information security manager might deploy to mobile network infrastructure. Khoumsi et al. (2018) revealed a couple of different types of firewalls; they all work differently but with the same objective.

One of the well-known forms of a firewall was the proxy-based firewall. A proxy-based firewall mainly acted as a conduit between the individual and the data (Tran & Ahn, 2017). In this case, the host device made a connection to the proxy-firewall, and the proxy firewall then made a special connection to the origin of the data (Tran & Ahn, 2017). The proxy firewall could inspect the data as it was being passed back and forth for any malicious data. Moreover, a proxy firewall's advantage was that devices outside the network could not gather information about the network. Proxy firewalls achieved masking the network because of the indirect connection (Nivethan & Papa, 2016). On the

other hand, the downside was that the delays and slowdowns could be annoying. Nivethan and Papa added that connections terminating connections and creating different connections could cause delays and degrade network performance.

Information security managers could have the option of deploying a stateful firewall too. This type of firewall would keep track of the information on connections, making it unnecessary to inspect each packet (Ghanbari et al., 2015). By maintaining these connections, stateful firewalls helped reduce data delay. Stateful firewalls maintain the connections due to the machines' identity from where the data was originating from, and this happened if the origin of the data was deemed legitimate (Salah et al., 2017). Furthermore, Salah et al. added that stateful firewalls reserved that state in the machine's memory once a connection was trusted, meaning that the firewall did not have to inspect the data originating from that machine.

Mobile devices do need some form of a firewall to mitigate external and internal attacks. Khoumsi et al. (2018) noted that the need for having firewalls on mobile devices could be beneficial as an added layer of defense. The utilization of host-based firewalls on mobile devices could complement the stateful firewalls deployed on the wired hardware. Tran and Ahn (2017) observed that host-based firewalls run on individual mobile devices. They are easier to configure than perimeter firewalls. Stateful firewalls offered protection from threats coming from within the organization's network, and they could help secure a set of applications and stop any suspect traffic completely. Disadvantages could arise with the utilization of host-based firewalls. Salah et al. (2017)

noted that host-based firewalls could be time-consuming due to the granular level needed due to configuration on many different servers for particular application sets.

Security managers do have the capability to train employees in the usage of firewalls. By training employees in the use and benefits of firewalls to secure the mobile network infrastructure, security managers would empower them. By empowering employees, security managers could also set outcome expectations. Outcome expectations remains a key tenet of social cognitive theory. Bandura (1998) argued that to reinforce a particular behavior, individuals must understand the behavior's potential outcome when repeated. By training and empowering employees on how to use and deploy firewalls, the security manager could reinforce the outcome expectation and encourage the continued use of firewalls in the organization.

Consequently, firewalls by themselves are a good strategy for information security managers. However, firewalls strengthened a network infrastructure when deployed within the defense-in-depth strategy and another defense-in-depth strategy element. One of those security strategies was the intrusion detection and prevention system.

IDPS

Intrusion detection and prevention systems could be a formidable security strategy when coupled with firewalls and encryption strategies under the defense-in-depth approach. Intrusion detection is the overall method of monitoring the organization's infrastructure and scrutinizing any signs of policy violations, incidents, or threats to the network infrastructure (Peng et al., 2016). Furthermore, the intrusion prevention system

worked actively to analyze intrusion detection and stop the network's perceived threats (Creech & Hu, 2014). The two systems worked together to form the basis of a network security strategy that information security managers could deploy. The system acts to weed out what hackers might target that could be important to the organization (Creech & Hu, 2014). Organizations are finding that IDPS could be a cornerstone of their network infrastructure security.

IDPS are continually looking and assessing mobile network infrastructure traffic. By being on a constant lookout, IDPS use different methodologies to perceive security incidents (Singh et al., 2015). One of the methodologies used was signature-based detection. Singh et al. noted that signature-based detection was whereby an IDPS compares signatures against detected events to identify incidents. It is the most basic detection method used.

Furthermore, the use of anomaly-based detection was vital. Anomaly-based detection compared regular activity to any suspicious activity for any significant deviation (Singh et al., 2015). Aljawarneh et al. (2018) observed that anomaly-based detection could effectively spot unknown threats to the network infrastructure. Another methodology that was utilized by the IDPS was the stateful protocol analysis. Aljawarneh et al. stated that the stateful protocol compares a predetermined profile of accepted classifications of individual state protocols against observed events for any signs of deviations. Firewall and encryption strategies could be instrumental, but IDPS strategy complemented both strategies and hardened security around the network infrastructure.

As network and data attacks have become sophisticated, information security managers are looking to mitigate attacks on mobile network infrastructures. Some information security managers using IDPS, in conjunction with other strategies, realized that you needed more than one strategy to mitigate attacks on network infrastructure (Peng et al., 2016). Many factors are making information security managers use IDPS as part of their strategy. Peng et al. observed that the quality of sophisticated phishing emails was getting better and more challenging for individuals or employees to detect by sight. Gupta et al. (2016) also observed that, when it came to sophisticated phishing, the authors stated that 91% of hacking started with a phishing campaign. Almost 30% of those phishing emails got opened by the targeted individual (Gupta et al., 2016). The use of IDPS could be pivotal when such cases arise. The utilization of IDPS could always be vigilant on what the users were clicking. If an employee or individual clicks on a malicious link, outbound traffic would get a flag as malicious (Jabez & Muthukumar, 2015). Mobile devices are also becoming ubiquitous in the workplace. Peng et al. stated that as devices connected to the network become more mobile, the more chances that a mobile device with a malicious infection like a virus or malware could connect to the network.

Maintaining a network infrastructure that spans many access points to other networks and private and public access could be challenging (Nejat & Kabiri, 2017). Challenges that organizations are facing also include having clients and customers who access the mobile network infrastructure. Due to having different types of data traffic, there are chances that malicious data could try to sneak through (Peng et al., 2016). Nejat

and Kabiri (2017) argued that attacks have become so sophisticated and could easily sneak through networks that are only protected by firewalls or encryption. IDPS could be a complementary strategy that information security managers could deploy together with their encryption and firewall security systems.

The combination of firewalls, encryption, and IDPS to protect the mobile network infrastructure is important. The use of IDPS on the mobile network helps monitor packets as they pass through the network itself. Also, having a host-based intrusion detection system on mobile devices was just as important (Peng et al., 2016). Host-based intrusion detection systems helped monitor that specific mobile device that houses the software. Singh et al. (2015) observed that HIDS software would monitor the device's key systems files to ensure that no unauthorized user was trying to circumvent the mobile devices system's security policy. One of the keyways that HIDS used to monitor a mobile device was through signature detection. Gupta et al. (2016) observed that the HIDS system could detect a deviation in the pattern of use and trigger a notification or shut down the traffic to and from the device using signature detection. HIDS systems could be instrumental as a second security layer for securing mobile devices connected to the mobile network infrastructure.

As the mobile network infrastructure becomes a target for different types of attacks, information security managers must find strategies that contained those attacks. The need to complement strategies with user understanding of the need and utilization of the IDPS could be fundamental when trying to help mitigate malicious attacks. Security managers could use social modeling to show the importance of using the IDPS, thus

reinforcing self-efficacy. Bandura (1998) noted that social modeling was necessary because an individual was provided with an identifiable model to demonstrate how to accomplish a behavior. Employees had to believe in their capabilities to use the IDPS to support mobile network infrastructure. Security of the mobile network infrastructure could also rely on another aspect of the defense-in-depth strategy; anti malware could help secure the mobile network infrastructure.

Anti Malware

The network infrastructure has become a vital communications backbone for many organizations, and as such, network infrastructures are becoming targets of different forms of malware and viruses. There has been a steady rise in malware that was not only directed to individuals but focusing more on organizations (Ucci et al., 2019). Ucci et al. also observed that there had been a large number of malware that targeted corporate organizations and government networks that connect to the internet. The recent statistics point to the fact that almost 80% of cyberattacks globally begin with malware infiltrating a network infrastructure (Ucci et al., 2019). Having a stout plan and strategy for mitigating such attacks was paramount to any information security manager.

Malware is a broader term that includes a host of computer codes, i.e., viruses, spyware, trojans, worms, etc., that have malicious intent on an individual or organization's data. The malware was designed mainly to harm computer networks and machines in that network (Tanaka et al., 2017). Malware does play an essential part in stealing data and as the foundation to start an attack on network infrastructure (Tanaka et al., 2017). Malware could come in different forms, i.e., as a script, executable file, or a

macros file. Due to their different types of variants that malware could come in, they might be devastating to network infrastructure (Yan et al., 2015). Ucci et al. (2019) stated that over 2.5 billion different malware targeted Windows machines might generate from existing malware samples. Malware propagates itself onto a network via a phishing email. Once an email with a malware code had been clicked and opened, the malware propagated itself onto the machine and lay low and avoids being detected (Al-Rimy et al., 2018). An attacker could gain access to the network by accessing the malware operating inside the network infrastructure. Malware and viruses could be devastatingly effective when an attacker wants to access network infrastructure.

Some organizations have become aware of the damage that malware could do to network infrastructure. The newer variant of malware have become more and more focused on organizations and has been devastating to those targeted (Jang et al., 2015). The need to have a mitigating strategy on malware was vital for every information security manager. Some information security managers deployed anti malware as a strategy to mitigate malware attacks on their network infrastructures (Blythe & Coventry, 2018). Anti malware software was becoming a mainstay in most organizations, and information security managers must know how to deploy them and how they function.

Individuals and organizations have used anti malware software to try and help curb the spread of malware. Anti malware software work in different ways to mitigate malware spread (Al-Rimy et al., 2018). Most anti malware software scans for malware using a database of known malware signatures (Blythe & Coventry, 2018). These delimitations dictate that the anti malware software could recognize and flag a potential

threat. With the rapid change of malware, the database had to be updated frequently. Another way that anti-malware software detected a malware threat was by using heuristics. Tanaka et al. (2017) observed that heuristics identified malware by how malware behaved and malware characteristics. Once an anti malware had identified a threat, that threat would be flagged. Most malware was quarantined or deleted, but some might cause more harm if deleted (Blythe & Coventry, 2018). For the malware that, if deleted, might cause more harm to the systems, anti-malware software would quarantine them to a safe storage place on a system (Blythe & Coventry, 2018). Anti malware software could be helpful to an information security manager as an added layer to other security strategies.

Anti malware was an important layer of security that security managers could deploy to protect the mobile network infrastructure. Anti-malware software could also be instrumental in protecting mobile devices from malicious software. Tanaka et al. (2017) indicated that mobile anti malware software could help scan downloaded applications to mobile devices for malware. They also helped curtail access to mobile websites that are known to spread malware. The use of anti malware on mobile devices was vital, but another aspect was also just as important, the user. Yan et al. (2015) stated that users had to be vigilant on how they used mobile devices; users had to be careful about what they clicked and which websites they patronized. The importance of users knowing how to navigate suspicious websites and coupled with antimalware software could help mitigate malware threats on mobile devices.

Security managers have the added responsibility of being the leader in a collective agency. Rubenstein et al. (2018) observed that collective agency in social cognitive theory dealt with the idea that individuals with the same purpose could achieve a common goal. Security managers could lead the charge in helping employees learn how to use and deploy anti malware software. The importance of employees understanding what they should keep an eye on when using anti malware software was also essential. By the security manager laying the groundwork and helping employees secure the mobile network infrastructure, they all achieved a collective agency. A collection agency could also permeate into different areas when everyone works together to secure the mobile network infrastructure. Authentication and authorization are areas where the collection agency could be important in the overall security of mobile network infrastructure.

Authentication and Authorization

Maintaining the confidentiality of the data passing through a mobile network was paramount for network security. Mobile network access is imperative to the people working in any organization and the clients served by that organization who might need access to that organization's data resources (Roozbahani & Azad, 2015). The need to protect the network infrastructure from individuals and devices that could spread malicious code was one of the core principles for any security manager. Having individuals and devices authenticated and authorized to use network resources was a privilege, and privilege had to be protected (Lo et al., 2017). Information security managers could deploy authentication and authorization as a means to know who was using the mobile network infrastructure.

Authentication could be a vital cornerstone of robust network security. As Amin et al. (2018) observed, authentication was the overall progression of recognizing a user's identity on a network. The need to use a set of recognized credentials unique to an individual was the essence of authentication (Amin et al., 2018). Authentication could recall the user's credentials and to be able to give them access to the network. Gokhale and Waghmare (2016) stated that the authentication mechanism usually resided in a database, and when a user submits their authentications, a comparison took place to make sure they are the proper unique authentication. Once the comparison had been compared and found to match, access was granted (Gokhale & Waghmare, 2016). The authentication process was simple and straight forward. The administrator gave a user id to an individual who was trying to access the resources of the network infrastructure; once the user inputted a user id, a comparison took place in a database; if it was true, the user got access; if not, access was denied (Mishra et al., 2015). Security managers could use authentication as one of the basic strategies coupled with other strategies to identify and mitigate unauthorized access to a mobile network infrastructure resource. By simply inputting a user id, it did not essentially mean that it was true. Thus, they had to prove their identity to access and grant rights to the network infrastructure (Gokhale & Waghmare, 2016).

On the other hand, authorization worked in tandem with authentication to give an authorized user access to network infrastructure resources. Hilia et al. (2017) stated that authorization was the action that occurred once the system authenticated a user. Once authentication took place, then the user was granted the right to access resources.

However, the user was authorized does not mean they had access to the whole network. As Gommans et al. (2015) observed, authorization was the system's ability to assess the rights granted to the user in the network infrastructure. Amin et al. (2018) observed that both authentication and authorization could be key to securing data from unauthorized users. Authentication and authorization are, in most cases, used in conjunction with each other. Although both authentication and authorization differ in concepts, they are critical to the network infrastructure in which users needed access to the network resources (Gommans et al., 2015). Organizations and information security managers would find that deploying authentication and authorization were beneficial and added security to the mobile network infrastructure.

The utilization of authentication and authorization as instruments that helped safeguard data was critical. Lo et al. (2017) observed that the need to have authentication and authorization mechanisms are important; they could be a formidable barrier to an individual with malicious intent if deployed correctly. Security managers had different ways that they could deploy authentication and authorization. Li et al. (2017) argued that security managers should use two-factor authentications on devices that individuals in the organization used. Lo et al. noted that two-factor authentications encompassed confirming a user's identity by using something they knew, i.e., a password; the other factor could be something they have, i.e., a key card. By deploying two-factor authentication, there was an added layer of security that goes in place to protect data. Also, Lo et al. stated that biometrics could be significant in protecting data. Security managers could deploy mobile software applications to mobile devices that could use

fingerprint scans, voice recognition, and retina scans to authenticate the user. Li et al. observed that user authentication and authorization mechanisms could play a huge part in protecting data from individuals who had malicious intent if deployed correctly.

Authentication and authorization could play a huge part in helping secure the mobile network infrastructure. Lo et al. (2017) observed that mobile devices, such as authentication and authorization, are important in mobile networks' overall security. The need to use mobile hardware tokens was essential for authentication and authorization as a mechanism (Amin et al., 2018). Mobile devices could be used as something you have, apart from something you know and something you are, which are cornerstones for authentication and authorization. Mishra et al. (2015) indicated that there are network access controls that utilized the use of a mobile media access control and internet protocol addresses as a form of authentication to a network. The use of MAC and IP addresses was another form of safely identifying who was on the mobile network infrastructure and if they are allowed to be there or not. Authentication and authorization could be crucial in how security managers managed and secured the mobile network infrastructure.

The inclusion of authentication and authorization plays part in the overall idea of how to manage and secure the mobile network infrastructure. Security managers could use authentication and authorization as a tool in concert with mobile network management to help protect the mobile network infrastructure. Teaching and instructing employees on utilizing authentication and authorization and letting them learn and use authentication and authorization properly helped improve overall self-efficacy.

Employees being able to adhere to the proper use in the long run of authentication and authorization methods fulfilled social cognitive theory's tenet of self-belief and proactive in what they learned (Bandura, 1998). In the long run, the need to utilize a multi layered strategy that merged authentication and authorization with the proper use was paramount to protecting the mobile network infrastructure and the applications that used the mobile network infrastructure.

Application Security

Applications form the other aspect of the mobile network infrastructure. In essence, applications are computer software programs that do specific functions on either a desktop or mobile device (Elsayed & Zulkernine, 2019). Elsayed and Zulkernine noted that both web and mobile applications helped organizations achieve essential business tasks that increase and measure their productivity. Therefore, applications' crucial role was to complete functions that assist the user's tasks and rendering to well-defined business rules.

Applications are essential in an organization's ecosystem, and this was because they are data conduits. Applications acted as middlemen for data in an organization. Bugliesi et al. (2017) observed that applications used a blend of server-side scripts and client-side scripts to present information, the storage, and retrieval of data, and therefore they had to be secured. Bugliesi et al. noted that application security's key elements are encryption, logging, and VPN. As applications are becoming ubiquitous, the need to have them secured was essential.

Application security on mobile devices was vital for security managers. Applications on mobile devices helped transform data that was consumed by users. Security managers had to make sure that those applications were secured. Elsayed and Zulkernine (2019) argued that applications must be secured to avoid data loss to malicious intent individuals. Security managers could help secure applications by using different strategies and methods. One of the key aspects of application security was encryption. Rawal (2018) argued that encryption had to be paramount in application security. Encryption scrambles data from the application and turns the data into unreadable text, and someone had to have the key to unscramble that data, or else they would not be able to read the text. Encryption could protect data from application to application and thus contributing to the confidentiality of the data.

On the other hand, security managers could implement appropriate logging for applications. Lazzez and Slimani (2015) argued that appropriate logging of what the application did was essential. By logging what the application does, if there were to be an exploit, security managers could pinpoint where and what happened to the application. Security patching done efficiently and quickly was vital for securing the mobile network infrastructure (Lazzez & Slimani, 2015). While logging helped security managers to be able to pinpoint when a problem happened, Le et al. (2018) argued that having an independent application audit was also a must. Le et al. observed that having a different set of eyes scrutinize the applications helped in the long run. The independent audits could ensure that the code in the deployed applications does what the code was supposed

to do. By doing an application audit, security managers could be confident that they deployed secure applications, and by that, they would be securing data.

Bugliesi et al. (2017) stated that security managers need to implement strategies that safeguard applications as a key component of securing data. Security managers could deploy encryption in the form of virtual private networks. Virtual private networks are a form of secure software that forms an encrypted tunnel that users could use to send data from application to application securely (Potey et al., 2016). By deploying encryption that encrypts data from application to application, data was protected end-to-end from prying eyes. Also, security managers could use logging of what the application is doing, and by that, streamline the application security. Logging using software that monitored what the applications were doing in real-time was important (Razzaq et al., 2014). As the software logged what was happening in real-time, security managers could figure out where a failure occurred and what caused the failure. Also, security managers could use a different opinion when auditing applications. Individuals or firms could carry out application audits; they should have no affiliation with the organization (Le et al., 2018). As the independent applications auditors scrutinize the code used and how they function, security managers could use the feedback to harden and secure the applications.

As security managers look for ways to ensure that applications are secured, they have to educate employees on using them. In social cognitive theory, an individual's capability plays an important role. The capability to learn and practice what one had learned was vital to retaining the acquired knowledge in the long run (Lin & Chang, 2018). Security managers had to stress the holistic importance of application security. By

teaching and training employees, security managers could reinforce the teachings by instituting vicarious capability. Lin and Chang observed that vicarious capability is what social cognitive theory identified as the ability for an individual to learn by observing actions and any consequences that could come as a result. By stressing the vitalness of application security and the costs of not following procedures to safeguard applications, security managers could help achieve overall mobile network infrastructure security.

Applications play a significant role in how data moves from the servers to what users see on their devices. Having applications that are secured should be one of the security manager's top priority. As security managers are continually looking for ways to secure applications, they are also trying to achieve a specific goal. That goal was to make sure that data was secured.

Data Security

Data security is another key element of mobile infrastructure. Data security refers to individuals' measures to protect and prevent unauthorized access to databases, websites, and computers (Wang et al., 2016). Wang et al. also argued that data security defended data from unintended or intended data corruption. Since data was one of the core aspects of the mobile network infrastructure, security managers must craft ways to protect data as it moves through the network or rests on databases. Zhang et al. (2017) observed three key data security elements: confidentiality, integrity, and availability. These three elements form the foundation of data security in any network infrastructure.

Confidentiality

Security managers have to look at the triad of confidentiality, integrity, and availability as the core elements of a robust security strategy to secure data. Through these elements, security managers could craft policies and procedures used by users to secure data (Tchernykh et al., 2019). Tchernykh et al. observed that confidentiality was among the first among equals in confidentiality, integrity, and availability. Confidentiality is considered the measures taken to protect data from unauthorized individuals (Colombo & Ferrari, 2015). Security managers had the task of making sure that the confidentiality of data was maintained. Security managers could maintain confidentiality by using different methods, including data encryption, passwords, two-factor authentications, etc. Colombo and Ferrari observed that by using data encryption methods, the user could only access the data that had been encoded by decrypting the data. The user had to have the key to decrypt the data; otherwise, the data looked like a random set of characters. By using encryption, data confidentiality was conserved.

On the other hand, passwords and two-factor authentications also play a role in data confidentiality. Tchernykh et al. (2019) observed that using a password and two-factor authentication maintained the data's privacy. If an individual needed to see or access the data, they had to furnish a username and password and add two-factor authentication. Two-factor authentication meant that the users had to utilize something they know, something they have, or something they are to access the data. Two-factor authentication could add another layer to the mobile network infrastructure by providing confidentiality to the data.

In data confidentiality, users of the data also have the responsibility of maintaining data confidentiality. Tchernykh et al. (2019) argued that users should take extra precautions when dealing and interacting with data to minimize data breach cases. Users should adhere to the policies and procedures that helped the organization protect data. By adhering to the policies and procedures of data security, data confidentiality could be maintained. Data confidentiality was a crucial part of data security, and it goes hand in hand with data integrity.

Integrity

Data integrity is another part of the key tenets of data security. Aldossary and Allen (2016) observed that data integrity involves the overall upkeep of accuracy, reliability, and data fidelity. Data integrity could be compromised as the data was in transit or at rest. Aldossary and Allen argued that data integrity must be unchanged and secure while in transport or at rest for data integrity to be warranted. For data integrity to be intact, there are elements that security managers had to take into account. Those elements are file permission, access control, version control, and cryptographic checksums. The responsibility to protect data integrity fell on all the users that use the data, but security managers had the overall responsibility to craft ways to protect data integrity.

Data integrity had to be protected by all appropriate means. Security managers could use several ways to protect data integrity. Zhou et al. (2018) argued that there are measures to safeguard data integrity. Measures to safeguard data integrity vary differently. Zhou et al. observed that security managers could institute measures like file

permissions and access control on the data. By instituting the use of file permissions and access control, security managers could manage who got to see data in particular files and who did not. The necessity to view or use the data files had to be paramount.

On the other hand, Garg and Bawa (2016) also argued that while file permissions and access control were essential, adding version control could form a sound data integrity security. Version control was vital for mitigating mistaken or accidental deletion of files. By instituting version control, the prevention of mistaken changes or accidental deletion was the goal. To change or delete data, an individual must follow version control steps, thus assuring data integrity.

Furthermore, Garg and Bawa (2016) added that security managers could include cryptographic checksums on the data to authenticate the data's veracity. Garg and Bawa noted that a cryptographic checksum was a mathematical value attached to a specific file. To verify the integrity of the data, an individual would use the mathematical value as a test. The need to add checksum would preserve the integrity of the data, and in any case, if the cryptographic checksum failed, the user would know not to trust the integrity of the data. The use of file permissions, access control, version control, and cryptographic checksum could be vital tools that could help with data integrity. Security managers had the latitude to use these strategies to protect data integrity as the data transverses through the mobile network infrastructure.

Security managers had to take responsibility for data integrity seriously. The maintenance, assurance, accuracy, and consistency of data are essential to organizations as a whole (Zhou et al., 2018). Security managers could utilize different methods to

achieve data integrity on the mobile network infrastructure. On the other hand, data confidentiality and data integrity had to be in sync with data availability to positively impact an organization.

Availability

Data availability plays an important role, just as data confidentiality and data integrity do in an organization. Aldossary and Allen (2016) noted that data availability denoted the capacity to ensure that users could access data when and where required within an organization. Data availability assured that the user would access the applications needed to perform their needed duties within the organization. The key elements that ensured data availability are software and hardware upgrades and repairs, redundancy, and adequate bandwidth availability. Security managers are responsible for ensuring that the mobile network infrastructure was always accessible by the users, thus guaranteeing data availability.

Security managers could ensure the availability of data by using different elements. To ensure that data availability was assured, security managers had to ensure that the hardware and software that helped run the mobile network infrastructure were maintained and functioned correctly (Thissen & Mason, 2019). Having the repairs done immediately or having replacement hardware could mitigate downtime whenever hardware failed. Also, the software was just as essential as hardware. The software had to be updated regularly and checked for viruses that could cause a network outage or slow it. By ensuring that hardware and software have the most recent updates, security managers could avoid any downtime.

Furthermore, by always making sure that the hardware was updated, data availability was assured. Also, Saxena and Agarwal (2018) added that the need to have hardware redundancy was crucial to maintain data availability. Having redundancy for servers, databases, etc., helped mitigate data availability whenever an issue occurred. Whenever a server failed, having a redundant server that can kick-in and came online, data availability would not be interrupted.

Additionally, Tan et al. (2018) viewed that the inclusion of adequate bandwidth and network bottleneck prevention was just as important. Adequate bandwidth had to be sufficient to allow the flow of data freely. If the data bandwidth were insufficient, there would be a risk that there would be a bottleneck when users tried to access the network and slow it. Data compromise could arise by having a network slow down and thus affecting data availability.

Data security had to be analyzed holistically whenever security managers had to implement safeguards. Security managers have the duty of helping employees learn and practice how to safeguard data. Social cognitive theory plays a vital role in this situation by utilizing social modeling and verbal persuasion. Security managers could help achieve the ultimate goal of safeguarding data and utilizing self-efficacy as a framework (Beauchamp et al., 2019). As data security encompasses data confidentiality, data integrity, and data availability, security managers could help employees understand and practice data security. Confidentiality, integrity, and data availability rules helped set the foundation for security managers to craft strategies to safeguard data on the mobile network infrastructure. Confidentiality, integrity, and availability are the core tenets that

every security policy had to have. The need to have policies and procedures that govern how data was used and protected was imperative.

Mobile Network Infrastructures Security Policies, Laws, and Regulations

As the mobile network gives employees and clients the ability to access the organization's resources from anywhere, there are also laws, regulations, and policies that have been constructed by government authorities, and the failure to follow those rules could lead to legal problems (Srinivas et al., 2019). Having these laws and regulations helped form an overall foundation of mobile network infrastructure, influencing how security managers crafted and established an organization's security policies. There are federal and state government rules that address such matters, but they are nonetheless not restricted to the Health Insurance Portability and Accountability Act, Electronic Communication Privacy Act, and Gramm-Leach-Bliley Act (Srinivas et al., 2019). Data must be protected all the time as the data moves through the mobile network infrastructure. Poullet (2018) stated that one of the main reasons that data had to be always protected was due to privacy and security concerns. Consequently, having laws and regulations set by governments that standardized data protection across the board was essential.

Information security policies and procedures compliance is a significant concern for many enterprises (Chen et al., 2015). Herath and Rao (2009) viewed that even with well-defined, clear, and detailed policies, there was a lack of compliance regarding employees following them. Furthermore, Chen et al. added that organizations had tried measures that included some form of punishment to dissuade employees from not

complying with security policies and procedures. However, there are still problems with security compliance. Understanding why individuals do not comply with policies and procedures was a foundational step to help seek a way to deal with this problem. Some factors played a role in leading an employee or a person's intent not to conform to information security policies and procedures. Herath and Rao carried out a research study to understand why individuals in an organization became non compliant regarding information security policies and procedures. Herath and Rao indicated that self-efficacy had a meaningful impact on information network security compliance. Additionally, Herath and Rao found out that having access to network resources substantially impacted an individual's self-efficacy.

Some researchers found out that when there was a negative interaction with security, there was a propensity to decrease security self-efficacy (Rhee et al., 2009). Additionally, Rhee et al. noted that individuals who had confidence in the technology and measures put in place were to control and mitigate threats had a sense of greater self-efficacy when it came to matters to do with security than those who did not. Therefore, security awareness could play a more significant part in security self-efficacy; this was because individuals who are more aware of security and procedures could help prevent and mitigate threats to the mobile network infrastructure.

How organizations handle access to the data on the mobile network infrastructure relies on the laws and regulations governed by the jurisdiction they are in and the policies set in place by the organization's security managers (Poullet, 2018). It was paramount that the security managers and everyone else who had access to and used the mobile

network know legal and regulatory issues regarding data protection (Clarke & Wigan, 2018). Depending on how far and wide the data moved, the legal and regulatory requirements could also change. Clarke and Wigan argued that if the data moved across international boundaries, the security manager must ensure that the protections adhere to that jurisdiction. Laws and regulations also played a big part in addressing issues that encompassed systems that are not secured well as data passed through those systems. Poullet observed that security managers had to consider and prepare well to protect the data. By having policies and laws that govern the mobile network infrastructure, data protection was always put at the forefront and guaranteed the data's confidentiality, integrity, and availability.

Laws and regulations of how data should be used and protected are the paramount responsibilities of the security manager and the employees. Employees have the privilege of using and interacting with that data. Flowerday and Tuyikeze (2016) observed that security managers must draft and implement procedures to adhere to the laws and regulations of protecting data. Implementing procedures that adhere to the law and regulations of protecting data came in many different ways. Flowerday and Tuyikeze argued that policies had to be realistic. There was no need to enact best practice policies if an organization cannot realistically support them (Flowerday & Tuyikeze, 2016). The other aspect was that the policies and procedures had to be made known in the organization. Bélanger et al. (2017) observed that policies that supported the laws and regulations should be well written and made available to everyone in the organization.

Nevertheless, one of the critical aspects that Bélanger et al. (2017) observed that would significantly impact self-efficacy was training. Training individuals in the policies, laws, and regulations created an impact whereby, when reinforced, and the training created the individual's psychological aspect to carry out the responsibility of enacting what they trained to do, using the procedures, laws, and regulations to protect data. Bélanger et al. also observed that what kept everything intact was the fact that security managers had to review the organization's policies and procedures and also to be able to enforce with consequences if users did not adhere to those policies. Making it clear that there are consequences to users if they did not follow policies and procedures, individuals would pay closer attention to them and learn how to carry them out.

The need to have and maintain policies, laws, and regulations that govern how individuals used and protected data was vital in an organization. However, security managers needed to ensure that only privileged individuals who needed to access the mobile network infrastructure had access to the network. For security managers to ensure that the mobile network infrastructure was secure, the need to look at security awareness to secure the mobile network infrastructure was vital.

Mobile Network Infrastructure Security Awareness

One of the critical aspects of looking beyond the technical aspect was the inclusion of security self-efficacy. The importance of understanding that small errors by users may lead to a larger effect security-wise was paramount (Mamonov & Benbunan-Fich, 2018). Understanding and being aware of the problems that can arise without the proper understanding of how network security operates by users could lead to severe

consequences. Mobile network security encompasses a holistic solution to all the involved parts, including an organization's policies and individuals using the network (Mamonov & Benbunan-Fich, 2018). Securing data that passed through the mobile network was a concern to the organization and the individuals using the network, which, by default, makes securing data a paramount objective for security managers.

Consequently, consideration should also be given to non-technical threats when addressing mobile network security. Tsohou et al. (2015) argued that there was a gap between an organization's awareness of security matters regarding mobile networks and the actual act of making sure the security issues got resolved. Acting on mobile network security problems could partake in a more considerable influence on implementing sound security policies.

Organizations influence how to enforce network security policies for their employees. Nevertheless, if those employees lacked adequate instructions on network security or data security procedures and they do not fully comprehend the impact of network security cognizance, there was a probability that those organizations could have a security incident (Tsohou et al., 2015). Security managers had to know and understand what the individuals using the mobile network understood about security. Gao et al. (2018) argued that employees could benefit from periodic testing to determine their network security knowledge level. Data security must be a paramount issue because the data passing through the mobile network must be protected (Gao et al., 2018). Some research showed that some employees might understand the network and data security; however, if their overall security awareness was nominal, then data assets could be

exposed to cyber threats (Gao et al., 2018). Mobile network security's importance had been proven more and more due to the breaches that affect mobile network infrastructures (Mamonov & Benbunan-Fich, 2018). Security managers play a vital part in ensuring that the organization's policies and procedures fit the overall data security strategies. Security managers had a key role in ensuring that deployed strategies can protect data assets on the mobile network infrastructure (Das & Khan, 2016).

One of the main concerns of a security manager revolved around the issue of overall security awareness. Bitton et al. (2018) led a research study to examine mobile device users' overall security cognizance in 17 different organizations based on how they use the mobile network and its security needs. Security managers had a unique perspective on addressing potential network security risks, threats, or attacks. Yao et al. (2018) also peered into the overall security practices and the impact of poor implementation on a mobile network. The research study focused on factors that could help cultivate security awareness to mitigate attacks and breaches within an organization. In this research study carried out by Bitton et al. the researchers approached 17 security managers of mid to large organizations. While both types of research focused on one objective, the variables were slightly different. Yao et al. focused on smaller organizations, while Bitton et al. focused on mid to large organizations. Yao et al. utilized behavior to understand the user's security awareness, while Bitton et al. focused on knowledge attitude and behavior as a catalyst to overall security awareness. Due to the numerous amounts of intrusions targeted towards mobile network infrastructures daily, security managers had to deploy security measures to mitigate those threats. One of the

key ingredients that could help in the fight to mitigate mobile network intrusions was security awareness, and security awareness could go a long way to protect data.

Security managers had to make security awareness a keystone to an overall understanding of how overall security functions. Implementing security awareness was paramount. Lynch and Mors (2019) argued that implementing a strategy was not easy, but the long-term effects can benefit an organization. One of the key elements of having a security awareness strategy was for the security manager to communicate the plan and how it lined up with the organization's general objective. Lynch and Mors stated that clear communication would help keep ambiguity at bay, and individuals knew what role they were supposed to perform. Security managers are instrumental in helping plan for security awareness, but they should also spearhead the training on security awareness. The training was crucial to reinforce what employees learned and also oversee the practicality of what they learned. Yao et al. (2018) also added that the need to track security awareness was essential. Security managers had to be able to track progress by different means to measure the progress of security awareness. One way to track security awareness could be by doing random checks on the employee's devices. Random checks also verify if employees follow what they learned and if what they learned was being translated to self-efficacy.

Mobile network infrastructure security awareness was critical, but it was one element that permeated into other different areas. Awareness comes to fruition when reinforced. One of the significant beliefs of social cognitive theory was reinforcement. Bandura (1998) stated that reinforcement could be positive or negative depending on the

reciprocal behavior and environment. Security managers should indulge in positive reinforcement regarding security awareness, and eventually, the outcomes are bound to be positive. The need to be always aware that the data passing through the mobile network infrastructure was essential and had to be protected could carry over to the mobile network security governance. When individuals are aware and know how to protect the data that is in their network, security governance helps further that cause.

Mobile Network Infrastructure Security Governance

Security managers play a huge role in ensuring that employees could execute their roles appropriately when it came to security. As self-efficacy was important, security managers need a framework to help them plan and execute the mobile network infrastructure's security governance. Moghadam and Colomo-Palacios (2018) observed that security governance encompassed the framework, supportive structure, and methods that offer assurance that the organizations' strategies align with their objectives. Security governance was also consistent with pertinent laws and regulations by observing policies and controls and could assign accountability to manage risk.

Security governance had to play a crucial part in how a security manager intended to protect data on the mobile network infrastructure. The ability to defend the mobile network was an integral part of protecting the data passing through the mobile network infrastructure. Venkatraman (2017) argued that a key objective for mobile network security was securing data on the network. Alreemy et al. (2016) believed that a key factor regarding mobile network security was the lack of knowledge on safeguarding the data while the data was on the mobile network. Mobile network security governance

warranted that data usage on the network adheres to the policies created, and all the data and devices are adequately secured (Zahadat et al., 2015). Mobile network security governance could be multifaceted because it involved many aspects of the organization. Mobile network security governance had to include, as a baseline, network control, and the measurement of how the system at large was managed (Zahadat et al., 2015). Mobile network security governance should focus on the technical aspects and encompass organizational matters and the cohesion among individuals needed to achieve the organization's objectives. The importance of establishing best practices for monitoring policies was foundational. Mobile network security governance pointed to a direction in which individuals who are using and protecting data on the network should follow (Venkatraman, 2017). A sound mobile network infrastructure design and how the network operates could be a vital aspect of the network's security success in general.

A mobile network security governance's efficacy could be observed holistically from the organization's perspective through its behaviors, beliefs, actions, and abilities. Mobile network security governance gives security managers the latitude to create security policies and implement those policies to protect data assets (Ali et al., 2015). On the other hand, Bermejo et al. (2014) observed that security managers could help organizations leverage data to streamline operations and also be able to secure data on the mobile network. Thus, mobile network security governance was important. Due to the involvement of different parts of the organization's network, security managers must create holistic risk management policies that enhance their business objectives (Ali et al., 2015). Mobile network security governance was a key component of safeguarding data as

the data transverses through the organization's mobile network. Since the main objective was to protect data, sound network security governance must be in place. Joshi et al. (2018) observed that an organization had to have a good network governance program in place; the program had to identify the risks to the network and assess them; they had to include both the technical aspect and the non technical aspect. Security managers should be able to spearhead the sharing of knowledge regarding the security risks to other individuals, thus making the rollout of network security governance plans easier to implement. A sound network security governance plan could give a security manager the latitude on how the mobile network security enmeshed together and how individuals in the organization should implement it. Joshi et al. argued that the network governance plan had to have flexibility due to technology changes from time to time. The plan had to be consistent enough to safeguard the mobile network.

As security managers draft mobile network security governance, they should also include the value of the policies they are implementing and how they would benefit the organization at large (Ali et al., 2015). To tackle security risks to the mobile network, they should craft an effective way of implementing written security policies. As the mobile network becomes a core component for organizations, the devices used to access the network need an effective mobile network governance policy (Zahadat et al., 2015). Security managers should be able to create sound network security policies, but they also had to be flexible enough to change as situations changed. When situations arose, and changes availed themselves, if the security policies are not flexible and did not have a robust framework, there are chances that the policies would not work. If security policies

fail, then there was a possibility that the mobile network might be open to individuals with ill intent. Joshi et al. (2018) described how security policies should be fashioned and employed in an organization in the greater security governance framework. Bermejo et al. (2014) observed that when there was an understanding of security governance policies in an organization, the benefits of capitalizing on a governance program to strengthen the security controls are a vital part. Security managers have to spread the knowledge and understanding of a sound security governance policy in an organization. Having employees understand the benefits of the policies put in place can effectively protect the confidentiality, integrity, and availability of the data passing through the mobile network infrastructure.

Mobile security governance helped put in place the framework needed to protect data throughout the organization's infrastructure. Mobile security governance is one piece of the puzzle that goes into forming a foundational structure of mobile network infrastructure security. Mobile network infrastructure management was another aspect that can help secure the mobile network infrastructure.

Mobile Network Infrastructure Management

Mobile network management was vital because its reliability depended on how the mobile network was maintained. Morato et al. (2018) observed that the network's reliability was a reasonable amount of time for the network to consistently deliver data packets from where they resided to the required destination. On the other hand, Söderholm et al. (2019) viewed that network management encompassed a broad range of purposes, procedures, and tools to administrate and protect a network. Mobile network

management had to be part of the overall security strategy to protect the network infrastructure. Manser et al. (2016) observed that mobile network management's core key element revolved around the notion of trust and control. Trust and control are critical in balancing and rebalancing the network (Söderholm et al., 2019). These two core elements complemented each other, network management could be grounded in trust, but control originated from monitoring and implementing measures to secure the mobile network infrastructure (Manser et al., 2016). Security managers should help cultivate trust and initiate control of how individuals could help with mobile network security. One key component of how to initiate trust was by encouraging self-efficacy. Bandura (1986) argued that self-efficacy was the belief in one self's ability to execute and achieve the planned goals. Security managers should help users know and understand their roles. Self-efficacy could help protect data on the mobile network infrastructure, and the belief in oneself could arise from the knowledge that individuals have learned. Some of that knowledge could come from security managers teaching users the implementation of techniques and tools needed to protect data on their mobile devices and the use of the mobile network infrastructure.

On the other hand, Hanus and Wu (2015) observed that security managers needed to manage the three core issues regarding security on mobile network infrastructure management awareness; those three core issues were phishing, passwords, and accidental oversights. Hanus and Wu argued that security managers had to help spread awareness on the effects of phishing emails and how they could be devastating if someone clicked on such an email. That email could contain ransomware that could spread through the entire

mobile network infrastructure and could be devastating. Security managers should help set up mechanisms that would help individuals create and save complex passwords. Chen et al. (2016) argued that having software applications that helped with complex passwords and also helped with two-factor authentications could help protect data. Hanus and Wu also observed that simple accidents could occur in an organization. There are chances that an individual would share something without knowing how sensitive that data might be. Training individuals on the importance of respecting and protecting data would be influential.

Implementing tools and techniques that could help protect data and the mobile network infrastructure must be at the forefront. Madlock (2018) argued that having a robust network management system before a network attack could help us know how to respond. Mobile network infrastructure could be attacked just like any other network, and those breaches could be devastating and time-consuming. Roozbahani and Azad (2015) stated that there are steps that a security manager could take to mitigate such issues. Since mobile networks and devices tend to connect away from the organization's wired infrastructure, users tended to use public or private wireless access to access the organization's resources. Security managers had to teach users how to use and deploy virtual private networks. Jingyao et al. (2019) observed that virtual private networks connected users separated by either geography or site remotely to their home or organization's network. Users should be proficient in how to deploy and use a virtual private network. Jingyao et al. argued that using a virtual private network could help protect data as it moved from a user's device to the home network. Security managers

should design and implement ways that users should learn and apply what they had learned regarding VPNs. By users being comfortable in deploying virtual private networks, that would be a step towards self-efficacy.

As mobile network management encompassed different aspects of protecting the mobile network, certain aspects are important. An emphasis on how to use and protect the software that is connecting everything is foundational. Software is a vital component of the mobile network infrastructure. Zota and Ciovica (2015) stated that software is comprehensive instructions that could regulate hardware operation. System software mainly encompassed programs that manage the hardware's resources, while on the other hand, application software was a program written with the user in mind (Zota & Ciovica, 2015). Security managers needed to increase software security self-efficacy for the users using the mobile software. Security managers needed to make sure that employees and users, in general, understand the risks that malware present on their mobile network infrastructure. Thornton (2018) argued that employees and users are the first lines of defense. Employees and users are the first to be targeted by malicious phishing emails; knowing how to avoid clicking on those emails was essential. Having users understand the consequences could also make it easier for them to learn how to use and protect the software that holds the data. Sen and Borle (2015) argued that with user empowerment coupled with the right tools, they could be instrumental in helping secure data and, in turn, secure the mobile network. Information security managers could empower users in different ways to be vigilant.

On the other hand, Morato et al. (2018) stated that information security managers could develop security best practices relevant to the users; information security managers should also provide adequate security protocols when training users. Morato et al. also stated that information security managers should show users that respecting their devices should be paramount for users to be empowered. The importance of users understanding how they browse and the sites they visit on their devices could affect the network at large was critical. Also, user participation in information on how to spot secured and unsecured websites was vital. Sen and Borle (2015) stated that the need to understand how to navigate secured and unsecured websites could be the difference between clicking a link that could load malware onto their devices. By putting this information together and teaching users how to spot a threat, information security managers would empower the user's self-efficacy. Users would be able to help protect the mobile network infrastructure in the long run.

In summary, some security managers had to find ways of protecting mobile network infrastructures and the data that was passing through the mobile network infrastructure. The inclusion of best design and practices was essential; they meet an organization's objective of cost-cutting and averting possible risk. The need to secure the mobile network infrastructure had to have different components working in tandem. Having a secure mobile network involves the security manager setting the groundwork with sound policies, the users educated on how to use and secure the network, and the users demonstrating how to do it, thus fulfilling self-efficacy.

Gap in The Literature

While there had been many research studies undertaken regarding mobile networks and the security issues surrounding the mobile network infrastructure, there was a lack of substantial research that encompassed the security of the mobile network infrastructure in developing countries, primarily focusing on Kenya. There is still a lack of substantial research on the security aspects of mobile network infrastructure in developing countries and the strategies that security managers deploy to secure those mobile network infrastructures. While some of the research studies have addressed some issues with mobile network security, some looked at the issue from a general perspective that addressed particular mobile networks. Yang (2018) identified issues regarding the mobile networks, but the issues that developing countries were facing concerning mobile network infrastructure security were many. The lack of adequate security in mobile network infrastructure in developing countries could be a haven for individuals with malicious intent (Okuku et al., 2015). As developing countries jumped the wired broadband straight to broadband wireless mobile networks, mobile network infrastructures' security was an issue.

Some of these developing countries, such as Kenya, are embracing the use of mobile network infrastructure. Okuku et al. (2015) observed that mobile networks speeds had risen exponentially in Kenya, while the security around the mobile network infrastructure lacked. Compared with other more developed nations, the emphasis on mobile infrastructure security and data security was prominent. Rathee et al. (2019) noted that organizations that use and deploy mobile network infrastructure have in place

standards that govern the use and deployment of VPNs, firewalls, data encryption, etc. The importance of using these strategies to safeguard the mobile network infrastructure and data was vital. Dye and Scarfone (2014) also observed that some major organizations such as the U.S Department of Defense had published publicly available standards that govern how mobile applications and data security in mobile network infrastructure fit in the holistic security structure of a mobile network. These standards enhanced the privacy and security of data as the data moves on the mobile network infrastructure. The protection of data on transit or at rest was also important. Hert and Papakonstantinou (2016) observed that the European Union implemented a stringent safeguard parameter for safeguarding data called the general data protection regulation. The law gives data protection, privacy to all citizens of the European Union and addresses the moving of that data outside the European Union borders. Yang (2018) noted that while most developing countries are still building and deploying mobile network infrastructures, there was a lack of data safeguard standards deployed in developing countries. Developed countries already had guidelines and standards on how mobile network infrastructure and data should be protected.

On the other hand, while some developing countries are catching up to the realm of mobile network infrastructure compared to other developed countries, there was still a need to build sound mobile network infrastructure. Ochang et al. (2016) found that developing countries, compared to developed countries, have had a jump start in both financing and technical development. Developed countries in the European Union and the United States have led to the development of the infrastructure that made mobile

communication possible. Ochang et al. observed that some developing countries in sub-Saharan Africa are trying to lay the foundations of mobile network infrastructure. Some countries in sub-Saharan Africa are trying to expand their mobile network infrastructure capabilities. Ben-Zeev (2018) found that Ghana used a mobile network infrastructure to help with mental health in rural areas. The country was rolling out mobile health initiatives centered around the mobile network infrastructure.

Compared with mobile network infrastructures in developed nations, developing countries are making small incremental steps that add up day by day. However, the overall emphasis had to be holistic. Developing countries and organizations that used those mobile network infrastructures should keep developing their infrastructures and include mobile network security as a cornerstone.

Due to the limited quantity of proficient published literature, there was a lack of literature focusing on this topic in Sub-Saharan Africa. Also, there was a lack of focus on methods and security strategies utilized to secure mobile network infrastructures in developing countries. I would be completing a qualitative case study that would focus on addressing and bringing forth the information that surrounds mobile network infrastructure security in developing countries. While using numerous databases for research (i.e., ProQuest, Science direct, Taylor and Francis, Ebsco, and Emerald Insight) and to explore the issue of mobile network infrastructure security in developing countries, there were no results that addressed that particular security issue. While I could not find literature that would directly support my research study, I could locate information on mobile network security and the security incidents on mobile networks in

general. By those results alone, there was evidence that there was a lack of information about my research study.

In terms of mobile network infrastructure, developing countries are eager to catch up with developed countries. Okuku et al. (2015) indicated that developing countries are moving fast to adopting mobile broadband networks, but the security was lacking. Finding peer-reviewed articles that spoke of mobile network infrastructure security in developing countries would have helped me address that gap in the literature. My research study would address mobile network infrastructure security in developing countries and how security managers in Kenya are securing mobile network infrastructures.

Transition and Summary

My core research study's resolve was to scrutinize the tactics utilized by security managers to protect mobile network infrastructures from cyber-attacks. This segment contained an overview of the problem of what security managers face in protecting mobile network infrastructures. The review of the literature was to increase the understanding of issues information security managers might face.

As a conceptual framework, self-efficacy, a vital part of social cognitive theory, provided a basis for exploring what motivated individuals to take security seriously or not comply with security policies. Security self-efficacy explained what might happen if individuals do not take security and policy compliance seriously. Thus, the lack of strategies that protected mobile network infrastructures could open the mobile network infrastructure to hacker attacks.

Section 2 provides the details and explained further the research methodology that suited this research. This section will expound on the research's role; it would set the criteria, compared the research approaches, and explored the population sampling, ethical research, data collection, analysis, reliability, and validity of the research study. In Section 3, I will present the research results based on a discussion of the data that I, as the researcher, collected.

Section 2: The Project

In this qualitative multiple case research study, I explored strategies that information security managers deployed to protect mobile network infrastructures in small to medium organizations in Kenya. This section includes a discussion of the study's resolution, a dialogue on the part of the scholar, as well as a description of the participants, the research approach and design used, the population and sampling, and ethical research as it pertains to the study. In this section, I also present the data collection method, the technique used to gather the data, the instruments used to collect the data, and data analysis procedures. The section concludes with a discussion of the reliability and validity of data.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies utilized by cybersecurity managers in Kenya to protect mobile network infrastructures from cyberattacks. The targeted population was cybersecurity managers in the Kenyan metropolitan cities of Nairobi and Mombasa. These two cities have the largest concentration of medium-to-large-sized organizations with information security managers. Out of the different organizations in these two large cities, I focused on four organizations that ranged from international non governmental organizations, telecommunication organizations, and government agencies to small- and medium-sized enterprises. These organizations had one or more cybersecurity managers that have implemented cybersecurity strategies to secure mobile network infrastructures from cyberattacks. The potential impact for social change included the probability of

decreasing the theft of important, confidential, or safeguarded individual or enterprise data. Furthermore, the application of cybersecurity strategies may lessen the loss of prospective identifiable data.

Role of the Researcher

When embarking on a research study, it is vital for a researcher to gather useful, quality data. When embarking on a qualitative case study, a researcher should collect information and data from different sources. Yin (2014) observed that the data sources could be archived data, interviews, observation, documentation, and current records. A researcher is the principal person who would collect the data and present the data in collected impartiality (Tomkinson, 2014). As the researcher in this qualitative case study research, my primary function was to be the principal data collection instrument. By being this instrument, I had the opportunity to organize and present the data collected. As a researcher, my core role was to recruit participants, conduct interviews with them, and collect and examine the data.

The researcher has the sole responsibility to make sure that the information they are putting forth is unbiased. The information that the researcher collects and analyzes should be free of bias so as to not affect the results of the research (Sohn et al., 2017). Since researchers are sometimes their own data collecting instruments, there is the possibility of bias permeating into the process of carrying out interviews (Roulston, 2016). At the time of the study, I had been involved in one capacity or the other in the IT arena for over 15 years. I had worked in environments where safeguarding the network was vital. I had dealt with security and network breaches, and this experience led me to

this research study on securing the mobile network infrastructure. My background and experience did not affect my neutrality when carrying out the interviews because I kept an open mind during the interviews and was cautious about the way I asked questions to not influence an interviewee to answer one way or the other.

As the researcher, I scrutinized and compiled the information that I gathered from the interviews. I presented the information as it was and did not misrepresent the collected information. While working on my research study, I reviewed *The Belmont Report* and its summary on ethical guidelines and principles on protecting individuals in a research study (see U.S. Department of Health & Human Services, 1979). *The Belmont Report* is a baseline description formulated by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research and printed in the Federal Register in 1979 (see U.S. Department of Health & Human Services, 1979). In the report, there are explanations regarding the anonymity, privacy, consent, and the safeguarding of data attained from the people participating in a research study.

In this research study, I presented the participants with consent forms that clarified that they had a sole right to opt out of the study at any given time if they chose to. I protected the individuals' privacy by not using their names and not sharing their information with other individuals who would be participating. All the data that I collected were always protected and secured due to the individuals' sensitive data.

I primarily used interviews to gather the information and data needed for the research. I used an interview protocol to help me organize the questions asked during the interviews. Reinecke et al. (2016) observed that an interview protocol helps a researcher

utilize a set of consistent interview queries that, in the end, deliver uniformity across the research study. As uniformity of questions was important in this research study, the correlation of the interview questions with the overall research study inquiry was significant. Castillo-Montoya (2016) observed that an interview protocol ensures that the interview questions align with the intended research study inquiry and helps minimize subconscious bias for the researcher. Dikko (2016) noted that using an interview protocol in an interview process helps add conformation to the interview process, reduce bias, and strengthen a research study's reliability and validity. I observed a strict interview protocol to gather data sufficiently and reduce personal bias in the current research study.

Participants

Focusing on individuals who provided quality information and data was vital for this study. The participants were information security managers working in small- to medium-sized national and international governmental organizations in the metropolitan cities of Nairobi and Mombasa. The inclusion criteria centered on the security manager's deployment and maintenance of strategies that mitigate attacks on the mobile network infrastructure in an organization for a minimum of 2 years. Once I received an email reply that included a completed consent form for the participant, I followed up them with a day and time for an interview.

For a robust research study to take place, there had to be a foundation with a good amount of data and data of good quality. Ben-Asher and Gonzalez (2015) observed that showing the eligible participants respect, conveying similar interests and relevancy, and having good research questions could be influential in the overall quality of an interview.

Hannon et al. (2016) noted that the informational strength of a study was related to the aspects of the participants' eligibility combined with focused sampling and sample size. Learmonth et al. (2016) also observed that the informational strength of a study encompassed its objective, an established theory, sample attentiveness, a set dialogue standard, and an analytical approach. To be included in this study, participants had to be security managers who had deployed security strategies to protect the mobile network infrastructure from cyberattacks. Due to this specific inclusion criterion, achieving the sample size of the research study could have posed a challenge.

After receiving approval to conduct the study from the Walden University Institutional Review Board (IRB), I contacted willing possible participants through overtly accessible sources and extended a request for their participation. They were informed that the study topic was the security strategies deployed by security managers to protect the mobile network infrastructure. In order to get access to the partakers, I used an email to communicate with the gatekeepers in the respective organizations, who ranged from upper management to human resources officers. Høyland et al. (2015) noted that having contact with eligible participants in a research study involved gatekeepers and observed that gatekeepers could help a researcher find suitable participants for a research study or hamper the research study contingent on how they perceived the study's value and eventual validity.

I established an ethical relationship while working on this study with both the participants and the gatekeepers. Understanding my role as a researcher was also beneficial. Thomas (2016) argued that a researcher who understood their holistic role of

certifying that the data collected were confidential and adhering to a strict participation protocol ensured that the participants were comfortable taking part in the study. Gehman et al. (2017) observed that having access to the participants and having the participating organizations disclose the data needed was important. After I was granted the needed access from the gatekeepers, I sent emails that contained a consent form to all the eligible participants. When participants replied with their consent, I followed up with a phone call and scheduled an interview.

Mcdermid et al. (2016) observed that having a good connection with the participants helped transparency and ease the interview process. Consequently, the email sent to participants containing the consent form also included a letter explaining the purpose of the research study and an appeal for the completed consent form before any interview occurred. Sorsa et al. (2015) noted that building a good rapport with the participants helped ensure good participation and positively influenced the data collected. Arsel (2017) also cited the need to have clear and concise communication between the researcher and the participants because this helped avoid ambiguity, leading to the collection of quality data. I had to consider my role as the interviewer and not only listen but also adhere to strict ethical research protocols.

Research Method and Design

In a research study, a researcher can utilize three distinct research methods: quantitative, qualitative, and mixed methods. All three methods have their strengths and weaknesses. The research method that a researcher chooses depends on which method best fits their criteria.

Method

In this qualitative study, my goal was to examine what strategies security managers used to secure mobile network infrastructures in the metropolitan areas of Nairobi and Mombasa in Kenya. Wilson et al. (2015) argued that the qualitative research method could be an analysis method that sincerely seeks to comprehend a social phenomenon within natural environs. Kozleski (2017) also noted that researchers deployed a qualitative method to examine an underlying concern in great detail and depth. A researcher can gather data for qualitative research in many ways to give a clearer picture of a phenomenon. Jagoda and Samaranayake (2017) noted that a qualitative research researcher could gather data by inquiring directly from the participants using questions that ask how and why. Analyzing data is also an important part of a qualitative research study. In analyzing data, Masta and Rosa (2019) observed that the qualitative research method does not center on the numerical aspect of data collection and analysis; however, the process helps gather and analyze information from various sources to form a single case study. Since my goal was to look at what strategies' security managers were deploying to protect mobile network infrastructures in Kenya, the qualitative approach was appropriate.

In this research study, there are a couple of other research methods that I could have utilized, quantitative and mixed-method research study. The quantitative research method focused on quantifying a particular issue using numerical data collected via polls, surveys, questionnaires, etc., or by using a pre existing set of statistical data using computational methods (Thomann & Maggetti, 2017). A quantitative research study has

an underlying foundation based on a hypothesis. It would also comprise how the researcher utilized measured data to prove or disapprove the research's hypothesis (Mccusker & Gunaydin, 2014). This research study did not intend to approve or disapprove a general hypothesis; in that case, the quantitative research method's use was not valid. The basis of a quantitative research study was the utilization of regression assessments to generate a thoughtful association between independent and dependent variables (Watson, 2015). A quantitative researcher gathers and examines data to establish a deduction grounded on statistical evidence that the researcher gathered, and the data would also be able to test a hypothesis or a theory (Almalki, 2016). In this research study, I did not intend to address the association dependence between dependent and independent variables to clarify technology dependence. This research study did not intend to examine a hypothesis; thus, the quantitative methodology was inappropriate.

The mixed method was not useful in this research study. The mixed-method research study intends to combine qualitative and quantitative methodologies to form a single research study (Mckim, 2016). The use of the mixed-method process dictated that researchers should coalesce the information attained by exploring complex variables and understanding the correlation between the attained information and the individuals participating in the research study (Yin, 2014). I chose not to use a mixed method in this research study because I might design two different research design methods to achieve my goal. Mccusker and Gunaydin (2014) noted that a researcher had to conduct two different research designs concurrently in a mixed-method study. One method would not give a clear picture of the study, and thus, the use of a mixed-method approach would not

suffice. However, Mckim observed that a researcher should deploy a mixed-method process when necessary, and the need arose to combine qualitative and quantitative methodology. However, this research study's core inquiry was suitable for the qualitative research method; thus, mixed methods were not ideal for this research study.

Research Design

Researchers can choose a research design study that would help answer the question that they are putting forward to study. I considered four different qualitative research designs, case study, ethnography, narrative, and phenomenological design in this research study. Nevertheless, the use of a multiple case design helped me as a researcher explore this study holistically and in-depth. Stake (1995) argued that using a multi case study research method would permit a researcher to explore and permit dissimilarities to be acknowledged. Collecting data from different sources helped give a more diverse picture of what the study was trying to explore. Yin (2014) observed that a case study research allows exploring questions, requiring collecting different information sources. Also, Yin and Campbell (2018) noted that when a researcher utilized a case study research, the researcher ideally gathered data from a couple of different sources, namely: (a) documentation, (b) archival record, (c) interviews, (d) site visits, (e) physical objects, and (f) observation. There was an added aspect of credibility for the study by collecting data from different sources and creating a case study. Houghton et al. (2015) viewed that a researcher who gathered data from diverse sources increased the research credibility and added credibility to the research study. The utilization of a case study gives the scholar the latitude to study a phenomenon without narrowing the research (Oreilly et al.,

2017). Therefore, the utilization of a multiple case study would be ideal for exploring the strategies that security managers were deploying to protect mobile network infrastructure from cyberattacks as a qualitative method design.

Another qualitative research design I would have used was the ethnography design. Ethnography research design allows researchers to display how cultures react, the communication between their community or within individuals, and the social implications (Jenkins, 2015). An ethnography research design would not be suitable for this study because it was not to observe a culture or a group and how they respond to security issues. The use of an ethnographic research study was useful when a study was endeavoring to determine cultural characteristics related to class, gender, and race for an examination of a particular group of individuals surrounding a specific criterion (Rashid et al., 2015). Using an ethnographic method, a researcher would have to witness the individuals participating for a prolonged timeframe (Rashid et al., 2015). I was not observing or researching individuals for a prolonged amount of time, so ethnography did not entail as part of my research study.

The usage of narrative research design could be pertinent to a researcher if the researcher were trying to scrutinize the partakers' historical experiences (Nassaji, 2015). Furthermore, Roux (2016) added that a narrative research design was a method of conferring what the participants had experienced in detail. The narrative research design also involved using the participant's storylines that categorized particular events, explicit activities, and causes (Bengtsson, 2016). The narrative research design did not fit this

study because I focused on strategies that security managers were using to protect the mobile network infrastructure and not focus on a person's life.

On the other hand, the phenomenological research design is a theoretical method regarding the cohesion of people who have gone through an experience that was not common (Crowther et al., 2016). Using a phenomenological research method typically required a bigger participant pool; consequently, this removed the need to placate the research study's sample size requirement. For research to have accurate results, the interviewer ought to have more than 15 participants when deploying a phenomenological research study (Sohn et al., 2017). Additionally, Adams and Manen (2017) viewed that a phenomenological research study was overall research on the human encounters observed through the person's view being affected by that phenomenon was their livelihood. I was not focusing on the phenomenon of the individuals participating, and thus, the phenomenological research design was not ideal for this research.

Population and Sampling

In order for a research study to be successful, population and sampling are the core foundation. By determining a locale and selecting the people who would partake in the study was imperative. The locale and the individuals participating depended on what information the researcher was trying to get and the research's goals to accomplish on the research study. I used a qualitative method and included a census sampling scheme to choose the individuals who participated in the research study.

This research aimed to explore what approaches security managers were using to protect mobile network infrastructure from cyberattacks. Sim et al. (2018) noted that the

importance of identifying partakers that furnished quality data and information that adheres to the research study overarching question was vital. To merge a good research population and quality, partakers were essential for a good research study outcome. Moser and Korstjens (2017) highlighted that well-rounded research questions could help select a good population that could give a rational perspective and produces quality data that reflected what the population knew about that particular study. Additionally, Fusch and Ness (2015) argued that when research questions are designed and inquired of different sets of partakers, data saturation was the goal. In this case, the utilization of total population sampling for the eligible partakers was key; partakers had a minimum of two years' experience in deploying strategies that safeguarded the mobile network infrastructure.

Since this research study explored what strategies security managers used to protect the mobile network infrastructure from cyberattacks, and the population was small, a census sampling method was ideal. Fatima et al. (2017) observed that total population sampling was a purposive sampling technique that encompassed an entire population. The examined population usually had specific characters and attributes. Fatima et al. noted that specific traits, knowledge, exposure, or skills that are not common could be a basis for using a total population sampling method for a research study. Also, Cajka et al. (2018) noted that as a unit of interest was very small, the need to use the total sampling method was ideal. Due to the sample size being small with unique characteristics, researchers had an in-depth study of their subjects. Some other sampling analyses are essential to account for in a research study. Sengupta (2016) argued that

sample size, a sample size area of inclusion or barring for participating, sample garnered that steers clear of bias, and ethical issues relating to consent was vital for a good research study. Also, case studies are unique in how they utilized population and sampling. Ellinger and Mcwhorter (2016) observed that case studies generally do not utilize numerical overview to take a broad view of a population, but as an alternative, utilized a logical overview to simplify a view towards a theory, thus utilizing sample size to be unique per study.

The essential utilization of a multi case study design could help a researcher decide that a premise was valid by responding to the *why* and *what* of a research question; consequently, the sample size of a study was not vital in attaining an in-depth and wealth of data of the study (Yin, 2014). To attain a wealth of data and in-depth analysis for this research study, I intended to contact at least four organizations or until I achieved saturation. These organizations differed in size; they ranged from international non governmental organizations, telecommunication organizations, government agencies, small to medium enterprises, etc., in both metropolitan cities. I presented the organizations as different cases, thus attaining a multiple case study. The number of partakers I intended to interview had one security manager per organization. If there were more than one, I intended to interview more partakers who could give me a holistic perspective of the strategies utilized to protect the mobile network infrastructure. I intended to interview eight partakers. Nevertheless, achieving data saturation was vital for determining the number of partakers I needed to achieve reliability and validity.

Data saturation is important in qualitative research. By having data saturation, a researcher conveyed that the data and information collected were abundant and complete. Fusch and Ness (2015) argued that data saturation occurred when no new information could be collected. A researcher could be confident that further data collection would yield similar results. Saunders et al. (2017) noted that a researcher could achieve data saturation by probing and asking a respondent to clarify their point; the respondent expounded on their point on a given response, clarifying what was not clear. Saunders et al. also noted that the importance of reviewing interview transcripts and requesting the respondent to clarify several points could achieve data saturation when the feedback becomes redundant. Additionally, Yin and Campbell (2018) found that a study achieved saturation when additional collected data did not contribute to the research study's new themes. As a researcher, I collected pertinent data until no new data or new themes occurred.

Partakers availability was a key determinant of how I conducted interviews. The interviews were via correspondence through skype, zoom video conferencing, and WhatsApp video messaging application; this was due to the potent transmission of the Covid-19 virus. The virus could be transmitted from individual to individual through close contact and respiratory droplets when an individual coughs, talks, or sneezes, which discouraged having a face to face meetings or face to face interviews. Morse (2015) observed that either face-to-face or video calls in interviews helped by watching for social cues. Social cues could be helpful for a researcher. A researcher could utilize social cues to help with a follow-up question to a partaker. This research study utilized a semi

structured interview format with additional follow-up questions to warrant a rich and in-depth collection of information and data.

Ethical Research

A researcher has an ethical responsibility to clarify the purpose of the research study, the role that the individuals participating would take, and how their information would be kept confidential (Strickland & Stoops, 2015). Before any of the data was collected, I attained authorization from the IRB at Walden University. When I attained approval from the IRB, under IRB approval number 04-22-20-0630739, I began the data collection course. A consent form that I used was sent by email to the individuals who were participating. In the email, I included a consent form that addressed any ethical apprehensions of the individuals participating, any risks that could occur, their sole right to refuse, or outright withdrawal from the research study whenever they wanted. I also instructed the individuals participating that their partaking was voluntary. For individuals participating in a research study, the importance of them knowing in advance how their information would be stored, disposed of and the length of storage time of the information was vital (Vitak et al., 2016). Before the interviews, I explained to the individuals participating that I would protect the data collected in a protected USB drive; I locked the USB drive inside a safe. After completing the research study, I would retain the data for five years, and consequently, after that period had passed, the USB drive would be destroyed by burning or shredding to pieces.

There was information about privacy and contact information concerning Walden University and me on the consent form researcher. The consent form also had

information advising the individuals participating in duplicating a copy if there were ever a need to refer to the form later. As the individuals got their consent forms, I advised them that they were under no commitment to partake in the research study. The importance of the individuals participating in the research study to understand that they could withdraw from the study without any objection was paramount (Allen & Wiles, 2015). In the consent form, I included information advising the participants that the study was voluntary, and they had the right to withdraw at any given time. To choose not to partake in the interview, individuals could choose to do so by email, telephone, or video call if in-person was not an option. Gainotti et al. (2016) observed that when a researcher used a financial incentive, there were chances that the researcher might get fabricated information. Manning (2017) observed that the use of compensation should be discouraged. There was no form of incentive offered to individuals partaking in my research study. I did not want the data I collect to be influenced by monetary compensation.

As a researcher, when directing a research study, addressing and verifying ethical issues is essential. IRB play an essential part in deciding if the study was on human participants; there had to be safeguards that addressed fundamental ethical problems that could arise (Crane & Broome, 2017). I did not contact participants before receiving IRB approval to certify that I followed clear ethical research procedures. Matters that regard ethics do have the capability of happening at any given time throughout a research study (Vitak et al., 2016). Before carrying out my research study, I did not set false hopes with the individuals participating in my research study. I did not offer nor request any data that

was not part of the study itself. I did not request the individual to share with me information that they were not comfortable sharing. Having safeguards in place that protect the subject matter, the analysis of the collected information, or the data collection itself was vital to protect against ethical problems (Mcdonald et al., 2016). All the data were stored and locked in a secure fire and waterproof safe, and the participants data were not to be shared.

The data collected - ranging from electronic, paper, or recordings regarding the interviews- stored safely in a locked safe that required a key. Organizations names and the individuals' names had to be protected (Vitak et al., 2016). Any form of documents containing the organizations or individual's data was locked when not being used. Documents or accompanying electronic media holding data about the individuals who partook in a research study would remain in securely protected custody for a minimum of five years for recovery impetus (Yin, 2014). All documentation was scanned and stored securely in a USB drive and secured with a strong password. I stored other documents warehoused in a secure cabinet. Subsequently, after the documentation's storage had passed, I would ensure that all paper documentation and electronic data are burned and shredded. Electronic media formats would be expunged, shredded, and burned. For a study to adhere to ethical standards, the researcher must act appropriately when defending the partakers from any form of maltreatment (Yin & Campbell, 2018). Throughout the research study, I held ethical guidelines and research policies in uppermost regard.

Data Collection

Instruments

I served as the principal instrument when conducting the interviews for this research study. Yin (2014) observed that as a researcher using a case study method, the researcher had the latitude to gather evidence from different sources. Those sources were observation – direct and participant, interviews, documents, archival records, and physical artifacts. As the principal instrument, I collected the needed information by conducting interviews and collecting the data from stored information. Researchers had to utilize the most important instrument, and that instrument was active listening while carrying out interviews (Twining et al., 2017). Being the principal instrument meant that I had to be unbiased when carrying out the research and leading the interviews. Dempsey et al. (2016) indicated that conducting a face-to-face interview may allow the interviewer to envisage the interviewee's body language when the interviewee replies to a question. While conducting the interview process, I paid attention to the interviewees for any physical body response that could allow me to ask a corresponding query. The absence of face-to-face could be a hamper to the interview process. Mcintosh and Morse (2015) observed that the absence of a face-to-face interview could lead to a poor rapport with the interviewee, causing a misunderstanding of questions and clarifying questions. I used open-ended questions in a semi structured interview for the face-to-face interviews for collecting data.

The advantage of doing a face-to-face interview allowed a participant to answer an already drafted question and have the latitude to chime in freely if there were any

additional information (Yin & Campbell, 2018). The sole determination of conducting interviews as a research tool was to survey the notions that information security managers had put in place strategies to secure mobile information infrastructures. A researcher should attain ethical guidelines during the interview progression to preserve the individual's privacy and increase the research validity during data collection (Lancaster, 2016). I ensured that the interview questions adhered to the ethical guidelines regarding interviewing individuals; this certified the validity, consistency, and dependability of all the individuals participating in the research study. Kallio et al. (2016) argued that interview questions should be crafted based on the holistic research question and the type of study. The interview queries were crafted based on the underlying research questions in the study. I presented the queries to the security managers, and they had the opportunity to convey issues that they had encountered while implementing security strategies on mobile network infrastructure.

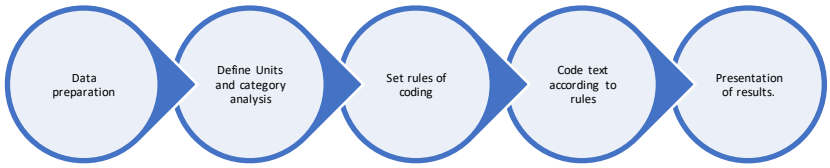
I requested access to collect archival data from the organizations participating in the research study. The archival data related to what had occurred to the organizations concerning security issues surrounding the mobile network infrastructure. Archival data could be beneficial. Thomson and Mcleod (2015) found that archived data was advantageous for academic theory; because the data was rich, researchers could compare the data using different methods. Yin (2014) also stated that archival data was vital and important as an ancillary source of data in a qualitative case study. The opportunity to collect archival data was beneficial because participants offered their knowledge

concerning the organization's data that might not be on public records (Bansal et al., 2018).

Content analysis is an integral part of qualitative research. Bengtsson (2016) noted that content analysis helped researchers dig deeper into the purpose and message derived from the data they collected. Content analysis was integral in quantifying particular words, phrases, and concepts in collected data (Bengtsson, 2016). The steps taken to utilize content analysis entirely are:

Figure 1

Content Analysis Steps



The foundation of content analysis starts with preparing the data that you want to analyze as a researcher. Erlingsson and Brysiewicz (2017) argued that the importance of transforming data before analysis began had to be stressed. The content had to be defined and correct. The next step was a researcher's definition of the units and category analysis used to analyze the collected data. Bengtsson (2016) stated that defining units and category analysis classified the collected data into themes that encompassed words, phrases, etc. Unit analysis and the emerging themes should be able to present an idea in the overall research study. The next step investigated the rules set for the coding of the

themes. Graneheim et al. (2017) observed that the importance of having clearly defined rules were vital with reliability. Having the rules recorded could help the researcher's method be open and reliable. The next step involved the coding of the texts according to the stated rules. Erlingsson and Brysiewicz stated that coding the data could be sorted and categorized by software or done manually. The coded data were categorized and recorded to appropriate units and themes. Lastly, the presentation of the results was the final step. Once the coding was complete, the researcher scrutinized the data to find patterns that emerged and concluded the researcher's research study question (Graneheim et al., 2017). Content analysis could be an essential tool for a researcher to utilize. A researcher could use content analysis to look deeper into the collected data, and content analysis could be instrumental in helping the researcher conclude their research question.

To strengthen the reliability and validity of the attained information from the participants, I used member checking and transcript review to go back to the interview outcomes. Birt et al. (2016) observed that member checking was a validation process whereby the accuracy of the information collected was checked based on previous data collected. Fenny et al. (2016) observed that transcript review was an integral part of helping the researcher validate the trustworthiness of the data they collected. By deploying both the member checking and transcript review process, I did a follow-up conversation to review and verify the information I had collected from the interviewee was correct. I attained confirmation with the participants to certify that the information that I gathered was correct based on the interview notes I had transcribed during the interview process. The member checking and transcript review process allowed the

individual who participated to have a chance to reflect on their own words and convey connotations additionally to their own words (Hadi & Closs, 2015).

Thomas (2016) noted that member checking was a key component used to validate, authenticate, or assess the reliability of data collected by a researcher. Fenny et al. (2016) affirmed that the research could have a second layer of validation and authentication of the data they collected by using transcript review. By using both member checking and transcript review, a researcher could also achieve saturation. Birt et al. (2016) argued that by using the first interview as a basis, the researcher schedules a second follow-up conversation for clarification, confirmation, and verification of what the respondent stated in the interview. The process repeats until no new themes or data emerged. Birt et al. also noted that a researcher could reach data saturation by using member checking and transcript review if the researcher's population were small. Member checking as a data saturation tool could be instrumental in a total population sampling method.

Member checking and transcript review also allowed the individual to advise me, the researcher, if there were any information that I might have transcribed erroneously during my transmission process. Member checking and transcript review are useful tools for initiating reliability; this was due to the information collected from subject matter experts, thus verifying quite a few more times to authenticate the data was key (Thomas, 2016). The key benefit of deploying member checking and transcript review was understanding the matter from an individual's viewpoint, adding value to the research study. On the other hand, the disadvantage of both member checking and transcript

reviews happened to be time-consuming. The follow-up conversations were required to satisfy the research study's member checking and transcript review aspects.

Data Collection Technique

As a researcher deploying a case study method, one should collect data from at least six different sources: participants and direct observation, interviews, documentation, stored records, and physical artifacts (Yin, 2014). As the researcher, before I collected any form of data, I had to attain a letter of collaboration from the individuals representing their organizations in the case study and IRB approval. After receiving an approved consent, I requested to work with the security managers in those organizations via email. After receiving positive feedback from the emails, I sent out consent forms, explaining what the study entailed. I also explained and advised the participants of their ability to withdraw at any time from the research study. Before the interviews occurred, I sent out reminder emails to the individuals participating in the interview. White and Hind (2015) observed that sending out reminder emails before the interview helps ensure that the individuals are available for the interviews.

I conducted face-to-face semi structured interviews. Semi structured interviews helped me as the researcher to focus more on the topic, which reduced the ability of the interviewee to go off-topic. A key disadvantage of utilizing a face-to-face interview is the prospect of a participant's availability, biases due to the data's alteration, and privacy concerns (Iacono et al., 2016). By getting in touch with the participants via email before the interview to remind them of the scheduled interview, I confirmed their availability. Before and during the interview, I also reminded them that their privacy was critical to

me as the researcher, and their privacy was paramount. Building a rapport with the interviewees is important, reflecting on their participation during the interviews (Vallano et al., 2015). I built a rapport with the interviewee and engaged in some general conversation before the interview. Weller (2017) noted that as interviewees offer information about their knowledge, a researcher could dig deeper into the information. I included about fifteen open-ended questions to the interviewees. The questions pertained to their knowledge and issues they have come across surrounding the security of mobile network infrastructure.

I recorded the interview process and responses, allowing me to review the information after the interviews. I completed reviewing notes that I took along with the recordings. The recordings directed me to address any information that could have required some clearness. Additionally, Smith and Mcgannon (2017) noted that member checking could help support the clarity of the data collected and help with collection techniques. I returned to the recordings now and then, coupled with the transcribed data with transcript reviews, to present a holistic depiction of the information gathered. In member checking and transcript review, the researcher requests the participants to review the transcripts to validate the collected data is accurate (Gunawan, 2015). I contacted the partakers to complete a follow-up conversation with each partaker and evaluated the information I attained during the interview process. By going back for a follow-up conversation, I gave the participants a chance to address whatever they saw fit regarding the information I had collected. Giving the participants the chance to address any inconsistency helped me achieve data saturation for the research study.

I worked with the security managers to attain archival statistics about the security problems they had encountered. Brown et al. (2015) found that there would be an increase in the study research's dependability by having different forms of data, making data triangulation a valued tool for research. The additional data would aid with data triangulation perspective by attaining archival data from the different organizations. On the other hand, Yin (2014) indicated obtaining historical data surrounding the "when, how, and who" that stored information could be valuable to a case study research. I tried and attained the stored information, which looked at former security practices implemented before, the obligations, and their utilities. I tried and attained data on the practices before any major security incidences, documented issues on paper, and solutions utilized for those issues. After obtaining those archival data, I reviewed the information and compared the present information on how security matters in the past affected the organization and how security managers handle those matters currently. Shortcomings could arise from a research study; these shortcomings usually emanate from the limited information and data (Cook et al., 2016). Although a data limitation could influence the studys' result, I used triangulation to gather and compare different aspects of the data.

Data Organization Techniques

For a successful research study, the storage of collected data had to be taken into consideration seriously. Being able to sort and organize data means that a researcher would locate and control access to that data. Throughout this research study, I leveraged diverse systems to organize data that I collected; this included but was not limited to

research trackers and logs, reflective journals, and classification systems. For each of the individuals participating in the research study, their information, data, and recordings were kept and stored separately. The recordings were kept separately in different locked folders in an encrypted USB thumb drive. Vitak et al. (2017) observed that a participant's information would help protect the data and information they afford by being able to confidentially cipher. I allocated each of the individuals participating with a unique code, and I kept the coding safeguarded in an excel document. The codes, in turn, were utilized in place of the individuals participating names to safeguard their data. To evaluate the information, I utilized the NVivo software. NVivo software can evaluate data to make the data understandable (Hays et al., 2016).

On the other hand, Alase (2017) argued that by having a research journal, there was a possibility that the knowledge you gathered will be available and shared readily. I had a research journal for the research study; it allowed for the information that I collected to be substantiated and for any follow-up research to be achieved and evaluated at any time. Additionally, Raterink (2016) noted that using a reflective journal could help a researcher identify the best framework to showcase a research study. Using a reflective journal, I identified a suitable framework and a participant pool suitable for the knowledge that I intended to extract for the study. I stored all the notes and data that I collected in an encrypted USB drive, and the documentation will be locked safely for five years.

Data Analysis Technique

For a research study to be holistic and successful, gathering, preparing, analyzing, and interpreting data was essential (Chowdhury, 2014). I utilized a qualitative multiple case study research method to analyze and present my research study. I utilized organizational triangulation concerning the data that I collected to increase validity and reliability. There was an advantage to the use of triangulation in a research study. Jentoft and Olsen (2017) observed the advantage of using triangulation: if there were an error in one of the sources of data, there would be a strong point in a different source of data to even out the error. By utilizing different data sources in my research study, I hoped to avoid some of a researcher's errors. The whole process of examining data involves the researcher sifting through the data, stripping the data, assembling the data, organizing the data, and ascertaining the relevance of the collected data (Chowdhury, 2014).

The examination of the collected data from a research study should focus on the exposure of important concepts that the data provided. The thematic analysis helped to uncover the important concepts in this research study. Wilson et al. (2016) indicated that thematic analysis encompassed vital qualitative study stages. The gaining of a complete comprehension of the collected data, the grouping of primary codes, unmasking of the themes that are in the collected data, having the familiarity of the themes, the enhancement of the themes, and the generating of a final study are the key stages in a thematic analysis.

The initial step of a thematic analysis starts with gaining a complete comprehension of the research study's collected data. Nowell et al. (2017) noted that

thematic analysis was an important method for identifying, organizing, and analyzing a study's theme from the data set collected. The data I analyzed included revising the interview transcripts, transcript review, and a thorough review of member checking the transcripts to understand the collected data. Any collected organizational documents were reviewed in the initial stage to gain a holistic comprehension of the organizations' policies and procedures as they related to devices that utilize the mobile network infrastructure. During a thorough review of the organizations' collected documents, taken notes helped with code generation. Chapman et al. (2015) also noted that interpreting the collected data in this stage would help generate codes and generate essential themes. The next stage outlined the process I used to code the collected data.

The next step on the thematic analysis included the grouping of the codes from the data collected. Coding concentrated on the words and phrases used that correlate with mobile network infrastructure security. The utilization of NVivo software helped with the coding of the collected data. After transcribing the interviews, coding commenced, thus assisting with dividing and grouping distinctive individual responses. A researcher could use the NVivo software to group themes, which, in turn, helped with analyzing the collected data. Maher et al. (2018) observed that coding was a crucial research tool because it helped discover themes in collected data. NVivo software would help categorize repeated themes in the study and link them with the participant's answers. Stuckey (2015) argued that axial coding in this stage could also be helpful to the researcher. Stuckey also stated that axial coding comprises connecting the collected data,

classifying the data, establishing the data categories, and recognizing the association amongst the recognized categories.

The next step after coding the data included the unmasking of the identified themes inside the coded data. Nowell et al. (2017) noted that the data collected had to be organized into themes using a coding technique. NVivo software could comprehensively help a researcher examine the research study data (Maher et al., 2018). Merging the collected codes into wide-ranging categories or utilizing themes while maintaining core themes' manifestations can be attained using the NVivo software. Constantinou et al. (2017) noted that the choice of themes during the analysis of the data stage was a vital task for a researcher. Constantinou et al. also stated that there are steps that a researcher could take to help in choosing themes. Those steps focus on repeated words by the participants, narrowing the themes down, developing a ranking of the themes, and linking the themes to the research study question and the research study's conceptual framework. The process delineated in this step helped generate themes for this research study. Thematic data analysis laid out how the themes were analyzed and connected to the literature review and the conceptual framework used in the study.

The next step of the thematic analysis of the data included familiarizing the revealed themes from the preceding step. Data collected were examined by utilizing the NVivo software; the themes that emerged connected to both the conceptual framework and the literature review. A study's conceptual framework should work in conjunction with the theory used, the literature, and the research study (Yin, 2014). Once the

researcher got the themes through the NVivo software, a complete analysis of the data to uncover the emerging themes was complete.

After connecting the themes to the conceptual framework, the next step entailed enhancing the collected themes. Percy et al. (2015) noted that after the researcher had finished coding, the next step was to look for the major themes. Major themes are, in essence, combined codes. Important themes could arise during this particular stage. Reviewing the regularity of the emerging themes and running a comparison to the themes via both the literature review and the conceptual framework revealed major themes. The use of major themes was evident from the participant's interviews.

The final step of the thematic analysis encompassed the creation of a comprehensive report. This report included both major and minor themes. The report showed the connection between the themes and the conceptual framework, and the research studys' literature review. The utilization of the NVivo software as a tool was significant due to its ability to create word maps and word clouds. The software helped with the collection analysis for the final statement of the research study. The presentation of discoveries was examined further in section three of this research study.

Reliability and Validity

Readers assign a value to a research study depending on their trust in the research study results. A researcher should certify that the information and data they attained for their research study was from reliable and valid resources. As the researcher, I must take the required phases to certify that this happens. A key resolve of a research study was to examine some unascertained information and the growth of information in some studies

that have are important to a particular topic. Shaw and Satalkar (2018) argued that the importance of accomplishing the research without any false data, fabricated data, or deception of data was essential when conducting research.

Reliability

The reliability of data was my key focus throughout this research study. Reliability was an element that had to be taken seriously from the commencement to the end of a research study. Leung (2015) observed that reliability was the assertion that the researcher's method was correct and was replicable at any given time. A research study course should be constant with what the researcher was intending or trying to study. For consistency to take shape, the beginning should have a research study question, the type of data collected, the collection of needed data, and the type of method utilized to analyze the collected data. Cypress (2017) noted that one of the key approaches of certifying reliability in a study was to ensure that the study process remained consistent throughout. Certifying that the information and data were collected correctly would ensure the collected data's duplicability (Tsai et al., 2016). When using a case study as a basis for a research study, the confirmation of reliability through a different researcher using the same procedure attained the same outcome (Yin, 2014). The confirmation of reliability by certifying the uniformity of the procedures used during the interviews was delineated.

Validity

By utilizing the case study research method, a researcher could utilize data triangulation to demonstrate a similar deduction, which increased the research's validity (Kelly et al., 2016). A Qualitative researcher searches to recognize methodological

strategies that may confirm the reliability of the researcher's discoveries. Trustworthiness correlates to the soundness of information attained from a reliable source, and it increases the unassailability of the study (Birt et al., 2016). Using member checking as a portion of response corroboration removed imprecisions. The individual participating stated what their qualifications were and their responses throughout the interviewing process. Member checking ensures validity toward the end of the research study by having the individuals partaking in the study review the collected information. Reviewing the information adds validity to the gathered data (Birt et al., 2016; Thomas, 2016)—attaining data from different sources certified validity by examining archived information and data from organizations and face-to-face interviews.

Dependability

The fidelity of the data a researcher collects and analyzes could be the foundation of a good qualitative research study. The information attained had to be comparable to the individual participants, and also, the data had to be detailed. Researchers have to maintain neutrality when examining the collected data. Lishner (2015) observed that for a research study to be dependable, a researcher must remain neutral while examining data, including sampling and analyzing the collected data. The use of member checking, when included in analyzing data, could increase dependability and credibility. Utilizing member checking permits partakers to validate the data, corroborating the data collected (Birt et al., 2016). Using member checking, a researcher could corroborate data saturation via no other coding, themes, or different data that may materialize (Birt et al., 2016; Thomas, 2016;). The documentation of the procedure for collecting the needed data was

essential, and this included recordings, interview procedures, and all the notes and documents collected during the research study.

Credibility

For a qualitative research study, credibility denoted an accurate depiction of information via explanation or account of an individual's experience (Kroeger et al., 2018). Utilizing member checking allowed the participants to authenticate the information and data collected, thus validating the gathered data (Birt et al., 2016). Hays et al. (2016) argued that member checking does allow participants to read a summary of the transcribed information, and they could certify the information accuracy, thus enhancing credibility. Throughout the interview process, I recorded the information and data to allow for a later review of that information. I used the same interview questions to ensure that the same decorum was enforced with all the individuals participating. Ensuring that the questions are uniform to all the participants added credibility and avoided skewing the study's information.

Transferability

In any research, transferability was vital. Colorafi and Evans (2016) indicated that transferability refers to the degree that a research study could transfer to other frameworks. On the other hand, Balmer et al. (2016) indicated that a researcher might boost transferability by using a total population sampling method. Also, Sarma (2015) observed that transferability could use a particular study and utilized those results in a different study. Maintaining a comprehensive and precise record of information and data gathered would prove transferability. Also, validating the information and data attained

through peer-reviewed sources would certify transferability. The data and information gathered could be substantiated; this, in turn, could permit other researchers to utilize the gathered data.

Confirmability

In order to ensure confirmability, all the individuals who partook in the research study reviewed the transcripts of the interviews. Reviewing the interviews confirmed that the information and data I collected were transcribed appropriately by reviewing the transcripts. Confirmability was also achieved by continually validating that the information and data gathered had been collected throughout the research study. Bush and Amechi (2019) noted that confirmability transpired by initiating and handling a succession of procedures that manage data gathering and data examination to the end of a research.

Additionally, Balmer et al. (2016) stated that confirmability could help show that research was trustworthy based on the partakers' perspective, the validation methods utilized, and the sources used for information and data gathering. Hays et al. (2016) also observed that confirmability as a thorough way to verify the goals delineated in a qualitative study. A researcher's ability to furnish information and data that could undergo scrutiny increased the validity of the information and data gathered.

Transition and Summary

This research study explored the strategies used by security managers in Kenya to protect mobile network infrastructure from cyberattacks. Section 1 covered the research problem, the purpose of the research, the study's nature, interview questions, the

framework used, and the literature review. The literature confined to Section 1 covered information and data regarding the research study correlated with accessing susceptibilities while using the organization's mobile network. The problems that had happened because of unsuitable security approaches and several studies that utilized the social cognitive theory corroborate the mobile network infrastructure affirmation. Section 2 contained comprehensive information reevaluating the purpose statement and also looking at the role of the researcher, the specifics of the participants, research method and design, population and sampling, collection of data (instruments, techniques, and organization), data analysis, and lastly, data reliability and validation techniques.

Section 3 encompasses the research study's synopsis, the research study's findings, the implications for social change, recommendations for action, and further study. Section 3 also includes the reflections of the research study in which I did confer my knowledge during the study process. Section 3 caps of this research study with a summary and the research study's deduction.

Section 3: Application to Professional Practice and Implications for Change

In this section, I provide a synopsis of the study and present the major themes revealed from data analysis. Additionally, this section includes a discussion of the implications for social change, the recommended action, areas of interest for further research, personal reflections, and the conclusion.

Overview of Study

The purpose of this qualitative multiple case study was to explore the strategies used by security managers in Kenya to protect mobile network infrastructures from cyberattacks. The data collected for this research study were from two main areas: semi structured interviews and documentation from the organizations. I conducted semi structured interviews with four security managers who worked for different organizations in Kenya. Additionally, I gathered and analyzed nine organizational documents. Every participant in the research study had experience deploying and implementing strategies that secured mobile network infrastructures. Each participant had no less than eight years of experience in the role of a security manager.

Four major themes surfaced from the data analysis in this qualitative multi case study: (a) security awareness and training, (b) infrastructure management tools, (c) defense-in-depth, and (d) security governance framework. The results of this research study align to the literature review findings. Furthermore, the findings of the current study corroborate Bandura's social cognitive theory as the foundational conceptual framework. In the following subsection, I discuss the four major themes in greater detail.

Presentation of the Findings

The core research question of this study was: What strategies do security managers in Kenya use to protect mobile network infrastructures from cyberattacks?

In this subsection, I unpack the four major themes found in this research study. I used methodological triangulation to evaluate the data collected from the semi structured interviews and the organizations' documentation related to the strategies used to protect mobile network infrastructures. I organized all the interview transcripts, transcript reviews in the form of member checking, and organizations' documents before uploading them into the NVivo software. NVivo software was able to help analyze and condense the data into four major themes: (a) security awareness and training, (b) infrastructure management tools, (c) defense-in-depth, and (d) security governance framework. Marshall and Wallace (2019) observed that software instruments such as NVivo let a researcher visually examine the data and code it into different themes.

In the following subsections, I present the major themes and compare them to the findings from the literature review. The themes are also linked back to Bandura's social cognitive theory. Table 1 displays the organizations as cases, participants, and documentation collected.

Table 1

Participants and Organizations

Organizations/Cases	Participants	Documents
Case 1	P1	D1, D2, D3
Case 2	P2	D4, D5
Case 3	P3	D6, D7, D8
Case 4	P4	D9, 10

Case references an organization, participants are labelled as P, and each organizations' document are labelled as D. Documents were labelled in ascending order from the first organization as D1 and the last organizations' documents were labelled D9, D10.

Theme 1: Security Awareness and Training

The first major theme to develop from data analysis was security awareness and security training in an organization. Security training and overall security awareness is the central line of defense in any organization. The core foundation of security training and security awareness in any organization lies in the belief that individuals must be well versed in knowledge and attitudes about information and data security. Each enterprise must take to account the importance of security awareness and security training. By utilizing security training and security awareness methods, an enterprise can reduce the likelihood of a data breach affecting the mobile network infrastructure. On the major theme of security awareness and training, there were four participants that were interviewed, and nine documents were analyzed. The theme of security awareness and training was referenced 16 times on both the documents and the interviews performed.

Participant 2 (P2) observed that security awareness and security training is crucial to their organization, and the emphasis starts from the moment a new employee is hired. Organizations can ensure that employees are always up to date with both security awareness and security training. Tsohou et al. (2015) indicated that organizations could utilize both education and constant practice to highlight the vital role employees play in protecting the mobile network infrastructure and the data that transverses through the network. According to P2, he stated on Document 4 (D4) that they rely on security awareness and training to ensure that employees know what to do when an incident occurs. P3 provided a different observation, stating that they rely on information security frameworks that have been put in place by the government to help them design systems

that are compatible with the suggested security frameworks. The organization's framework has to be in alignment with the government's policies to protect data. P3 reported that data security is mandated by the government and having well-informed and trained employees is essential.

P1 also observed that information and data security training is crucial for organizations. P1 observed on D1 that security managers must ensure that a security awareness culture is cultivated and supported throughout the organization. Emphasizing the need for security awareness and security training is vital to organizations. Training could help information security managers ensure that mobile network infrastructures are secured.

Additionally, according to P2, every employee in their organization must fulfill two security awareness and security training sessions in a calendar year. On D2, P2 disclosed that employees' perceptions of information security changed when there was a mandate for security training; employees must sign a digital copy of documents showing that they attended both security meetings offered each year. The digitally signed documents go into the employees' files in the human resources office.. P4 also discussed security training in their organization, stating that, once the security training is over, all employees must sign that they have read and understood what was taught in the security training sessions and understand the organization's information security policies. The participants' interviews responses aligned with how organizations could utilize both education and constant practice to highlight the vital role employees play in protecting the mobile network infrastructure. P4 reiterated that a positive approach toward

information security is attainable through proper security awareness, training, and security education.

The theme of security awareness and security training is an essential strategy for protecting mobile network infrastructure and the data that travels on the network. Previous studies conducted on securing mobile networks supported the participants' responses to the interview questions in the current study. According to Gao et al. (2018), implementing an efficient and thorough information security program starts with establishing security awareness encompassing information and data security. According to P3, each organization must look at information security as necessary to their organization. P1 stated that having employees who are well trained and aware is key to minimizing breaches to their mobile network infrastructure. At the core of information security awareness is the idea that what everyone does in the organization can mitigate the risk of breaches. The individual's focus as the front line, and not the devices themselves, is essential in reducing network breaches. The critical objective of security awareness in an organization is to foster a culture that embraces information security.

The theme of security awareness and security training aligned well with the social cognitive theory. One of the core principles of social cognitive theory is the concept of self-efficacy (Honicke and Broadbent, 2016). Honicke and Broadbent referred to self-efficacy as a person's ability to judge their capabilities to self-organize and be competent executing a plan required to achieve the desired performance. Self-efficacy should be at the forefront when designing a training system or an awareness program. As observed earlier, for an organization to have a robust information security culture, the organization

must invest in the people who utilize that network regularly. By the organization investing in individuals using the network, the organization helps cultivate a security awareness culture. P2 stated that when it comes to the organizational analysis of information security, they decided to focus on employee awareness and ensure that each employee has the right tools and knowledge. By empowering employees to know and act with informed knowledge on protecting the mobile network infrastructure, they cultivated their employees' self-efficacy.

The study results indicated the importance of maintaining a grounded culture of security awareness and security training. One fundamental approach to boosting security awareness in an organization is to establish a culture of security. Bitton et al. (2018) described a security culture as an individual's awareness of the shared principles and values among other individuals in a work environment. As stated by P2, the security culture they have cultivated in their organization is robust, and the organization has seen the fruits of that culture. The employees are always vigilant of security breaches, which has helped the organization be a security-first environment. Das and Khan (2016) stated that a holistic security culture in an organization must start with the individuals who regularly use the network, and those individuals are the employees. Changing a single employee's behavior can be challenging; however, if the whole organization has a structure and cultivates a security culture, individuals will influence other individuals to maintain that culture.

Theme 2: Infrastructure Management Tools

The second emergent themewas infrastructure management tools. This theme centered on how organizations must use tools at their disposal to safeguard the security of their digital assets. The constantly changing technological environment implies that organizations should take a practical stance when it comes to security. Organizations ought to make sure that they keep up with new trends, threats to their network, and new vulnerabilities. The introduction of mobile devices onto any organization's mobile network infrastructure demands tools that the organization can use to manage those mobile devices. When appropriately utilized, technology management tools can help mitigate data breaches that emanate from mobile devices. On the major theme of infrastructure management tools, there were four participants that were interviewed, and nine documents that were analyzed. The theme of infrastructure management tools was referenced 55 times on both the documents and the interviews performed.

All the participants observed that their organizations utilize different technology management tools to safeguard their mobile network infrastructure. In this subsection, I further examine some of the management tools used by organizations to manage their mobile network infrastructure. According to P1, P2, and P4, their organizations utilize mobile network infrastructure management tools to safeguard their digital assets from external and internal threats. P4 remarked that the mobile infrastructure management software tool that the organization uses is a crucial part of the information security infrastructure. P4 stated that network infrastructure management software gives them the ability to monitor the network's mobile devices.

P2 stated that the use of technology management tools helps the organization safeguard mobile hardware devices, explaining that "if one or more of the devices are either lost or stolen, the management software gives them the ability to shut the device down and wipe the device's drive of all the data and render the device useless." P4 also observed that knowing that you can wipe out a device that is lost or stolen remotely is essential to protecting data. P1 noted that the mobile network infrastructure management software is a cornerstone tool that organizations can utilize to monitor mobile devices accessing the mobile network infrastructure. According to P1, they have deployed Cisco Meraki as their network infrastructure management tool to manage mobile devices in their organization's network. P1 remarked that "Cisco Meraki gives them the flexibility to have the whole network on a single dashboard and having the means to administer security policies, perform remote functions, and remote troubleshooting many devices from a single dashboard is a good thing." Most of the individuals who participated in the study agreed on the importance of management tools.

To have infrastructure management tools that align with organizational needs is vital. Infrastructure management tools help the organization to be able to oversee, observe, and ensure that the mobile devices that are connecting to the mobile network and used by authorized employees (Hanus & Wu, 2015). P3 noted that the infrastructure management tools they have deployed in their mobile network infrastructure are robust. P3 also stated that infrastructure management tools do possess the capability of letting the security manager monitor the devices logging into the mobile network. On the other hand, P1 mentioned that having management tools gives the security manager the ability

to shut down and render a company-issued device useless if stolen or lost. In essence, security managers have to adapt to the fact that organizational data in this day and age may reside beyond the organization's home network's confines. Security managers need to have a system that can help them manage those devices. An infrastructure management tool is ideal for such situations for security managers.

Infrastructure management tools theme aligned well with social cognitive theory, which functioned as the conceptual framework for this research study. Mamonov and Benbunan-Fich (2018) noted that social cognitive theory centers on the individual being empowered and equipped with adequate knowledge to rely on their confidence to execute a task. Organizations must rely on individuals to carry out important information security tasks in an ever-changing information technology environment. Security managers rely on individuals who have been trained and equipped with the knowledge of how to utilize tools to protect both organizational devices and data. These individuals use their training and knowledge to help secure the mobile network infrastructure. Security managers who use the social cognitive theory with self-efficacy as a basis for their security approach have a specific intention to concentrate on the individual as the gatekeeper and empowering them with tools to protect the mobile network infrastructure. By empowering the gatekeeper, this enables them to make the right decisions when the need arises.

Based on this research study's discoveries, having robust infrastructure management tools will accommodate each element needed to secure the mobile network infrastructure. It will also align them with the demands of the organization. To achieve

this, security managers must consider a holistic view of their organization's information security, including the tools needed to help secure the mobile network and the data that flows on it. An organization also needs other components to work together to maintain a high standard of security. Security managers need to utilize a well-grounded defense-in-depth strategy. A well thought out layered defense strategy can be instrumental in helping secure the mobile network infrastructure. In principle, security managers must look at the organization as people-centric first and equip them with knowledge and tools to secure the mobile network infrastructure. The organization's overall objective is to ensure the network and the data are secured. Security managers should use the best infrastructure management tools available and well informed and knowledgeable individuals to help secure the data and the organizations' network.

Theme 3: Defense-in-Depth

The third major theme that arose during the analysis of the collected data from the research study was the notion of defense-in-depth. The preface behind the major theme of defense-in-depth is that it encompasses a holistic view of the organization's mobile network infrastructure security and the devices that access that network. Jander et al. (2018) observed that a security manager intends to use a layered approach to secure the mobile network infrastructure by utilizing a defense-in-depth strategy. This research study's discoveries, combined with the present literature, support this major theme, and point out that defense-in-depth is an essential strategy in mitigating data breaches on the mobile network infrastructure. On the major theme of defense-in-depth, there were four participants that were interviewed, and nine documents that were analyzed. The theme of

defense-in-depth was referenced 148 times on both the documents and the interviews performed.

All the participants of this research study emphasized the importance of utilizing a defense-in-depth approach to their mobile network infrastructure. According to P4, the strategy they use comprises different layers and has several security team members that monitor the mobile network infrastructure. According to P1, the objective is to protect every element of the organization's mobile network if there is an attack. P1 stated that "if there is an attack, there is a documented plan for dealing with the perceived attack, and what individuals should do to help mitigate the attack." P2 and P3 indicated that even though they have not encountered a massive network or data breach yet, there had been cases that were caught earlier due to the defense-in-depth strategy utilization. Three of the organizations' D2, D7, and D10 documentation studied for this research study refers to utilizing the defense-in-depth strategy; the documents pointed to the use of firewalls, virtual private networks, physical security, among other forms of security deployed.

The organization's defense-in-depth strategy are plans that utilize the resources available to mitigate internal and external attacks on the organization's mobile network and data assets. According to P1, their organization undergoes a review of the documents concerning the deployment and utilization of the defense-in-depth strategy every six months. According to P1, "the review ensures that the documentation is in alignment with the strategic needs of the organization." P4 also mentioned that by having documented plans of deploying and using defense-in-depth strategies, his organization could react to an incident quickly and precisely. P4 stated that "the documents also map

out how to protect all the mobile network infrastructure components using the defense-in-depth method." A defense-in-depth approach could help security managers mitigate data breaches on mobile network infrastructures.

Securing the mobile network infrastructure by looking at the components that access the network and the accommodations they need to ensure access is essential to any organization. P3 observed that individuals who also use the mobile network with their devices need to be secured. All the individuals who participated in this research study agreed that we have to look at the network's wholeness and remember that smaller parts of the network combined make the more extensive network. Jander et al. (2018) argued that we must look at the mobile network infrastructure as an ecosystem; different ecosystem components must have synergy. P1 stated that, due to having different devices accessing the mobile network infrastructure, having a layered defense helps ensure that all these different devices are secured. Jander et al. stated that to protect the mobile network infrastructure, security managers must consider all the different devices that access that network and form a layered security approach that aligns with its business objectives.

The organizations that use a defense-in-depth method to secure their network follow one of the foundational social cognitive theory tenets, self-efficacy. Employees utilize the mobile network infrastructure and mobile devices that access the network. Security managers train employees to be efficient and confident in using the devices and secure them properly. By employees executing the roles of learning how to and being able to do everything by themselves, they fulfill one of the fundamental tenets of social

cognitive theory, self-efficacy. Conferring to P3, security managers have to teach the individuals who are using the devices. Those individuals must use the devices well and protect the devices and the data in those devices. Bandura (1999) observed that self-efficacy is not what skill an individual possesses, but what that individual does with that skill is essential, also, the ability to judge and the aptitude to establish and implement a course of action to achieve a selected goal that is paramount. In essence, to have a robust defense-in-depth strategy for defending the mobile network infrastructure, the most important aspect must be the people. Security managers should train employees on how to use and maintain the different layers of the defense-in-depth strategy.

Based on this research study's discoveries, a sound defense-in-depth strategy will accommodate each element needed to secure the mobile network infrastructure. The defense-in-depth approach also must align with the demands of the organization. To achieve this, security managers must consider a holistic view of their organization's information security, empowering their employees as a focal point. Sarika et al. (2016) argued that organizations must design their mobile network security systems by utilizing the layered method. Using a layered design to network security helps security managers create an overlap to the security measures. If one of the security measures fails, another one can take over seamlessly. Having a defense in depth strategy is fundamental in any organization that wants to secure its digital assets.

Theme 4: Security Governance Framework

The information security governance framework's major theme emerged through the data analysis done for this research study. A vital part of any organization's business

objective and information technology strategy is network and data safeguard. Security managers should prioritize the protection of the mobile network and the digital assets in that network, and the devices that access that network (Potey et al., 2016). Every organization must ensure that its information governance framework includes policies, procedures, roles, and metrics aligned with the organizational business objectives. Moreover, the security governance framework structure must encompass every digital asset and the devices the organization has authorized to access its mobile network infrastructure. On the major theme of security governance framework, there were four participants that were interviewed, and nine documents that were analyzed. The theme of security governance framework was referenced 57 times on both the documents and the interviews performed.

An organization's security governance framework forms how individuals in the organization will deal with information security and the digital assets that the organization controls, according to P3. There are different types of policies that an organization can implement depending on its business objectives and the data they own. The consensus among all the participants was that having good policies, procedures, and metrics is essential. P2 disclosed that among other policies that their organization has included.

- end-user policy,
- access control policy,
- encryption policy and
- information security policy.

On the other hand, P2 stated that the security manager's goal and the organization are to ensure that a security breach does not occur. P2 stated that having policies and procedures ensures that an organization will be prepared for an incident if it happened. The vital point with any successful organization is preparedness. P3 observed that most security managers sometimes do not consider the organization's overall footprint when designing the organization's policies and procedures for security, leading to a mistake in data or network security. Technology keeps evolving at a fast pace, and organizations must also evolve as fast too. The basis of a good information governance framework starts with having well-designed policies and procedures, according to P1. As mobile devices are becoming a mainstay in most organizations, security managers must balance the need for the devices to access the mobile network infrastructure and the security threat they might pose to the mobile network infrastructure. According to P2, the organization distributes a memo every fortnight to all employees outlining any new security threats to their mobile network. In that memo, P2 also stated that the security manager emphasizes and encourages employees to refer to the organization's security policies and procedures related to security incidents.

All participants in the research study agreed that any organization's success hinges on its information security strategy. All the participants agreed that there could be security lapses. P1 stressed that if the organization's policies and procedures do not align with its business objectives, then a security lapse or breach may occur. Srinivas et al. (2019) argued that safeguarding the organization's data assets begins with the correct application of all-inclusive security policies and procedures. As agreed by the research

study participants, an organization's security policies and procedures establish a good foundation of data and network security. They must focus on the overall organization's footprint. Poullet (2018) noted that organizations fail to properly implement good security policies and procedures to their security model. By that, those organizations can put their digital assets at risk. As noted by P2, network and data breaches sometimes occur due to organizations failing to manage their data assets effectively using policies and procedures in the greater security governance framework.

When perceived through the lens of social cognitive theory, an organization with a well-rounded security governance framework that includes policies and procedures can promote overall success in that organization. Bélanger et al. (2017) noted that when policies and procedures do not get enforced, there is bound to be a breakdown, and that breakdown might result in a network or data breach. Employees must learn about the organization's policies and procedures. Those employees must attain confidence in executing, following, and maintaining the organization's security policies and procedures. By performing their roles independently, employees project the essence of self-efficacy, a social cognitive theory tenet. Security training will help employees be comfortable executing their roles, for example, to be comfortable in following rules for strong password policies and procedures and to be able to generate strong passwords to mitigate password guessing attacks on their login screens.

As organizations also enforce the use of policies and procedures, employees can learn from other employees too. By learning from others how to follow the policies and procedures in place, employees may attain social modeling. Social modeling is a tenet of

Social cognitive theory too. Aunger and Curtis (2016) noted that people could learn by seeing and following what other individuals are doing. Social modeling can be powerful when it comes to expectations from the organizations to employees regarding policies and procedures. New employees learning from other employees who have been in the organization for some time on approaching and maintaining acceptable security standards can set a good foundation for those new employees. Organizations that leverage social modeling can collectively improve how employees view and interact with security policies and procedures and improve network and data security.

Implications for Social Change

This research study revealed that there could be some improvements made to strategies utilized by security managers to mitigate breaches to the mobile network infrastructure. Mitigation can lead to a reduction in the number of violations that affect organizations in developing countries. The key implications of social change for this research study lie in the fact that, by deploying the strategies discovered in this study, mobile network infrastructures will be secure. Security managers will help mitigate data breaches and protect sensitive customer data from being exposed.

The findings of this research study may help with securing organizational data. Apart from the breaches to the mobile network infrastructure, data breaches can also occur in organizations. By utilizing strategies discovered in this research study, social change implications will help security managers plan adequately to secure organizational data. Data breaches as a result of insecure mobile network infrastructure may also lead to data corruption. These breaches can directly affect an organization's bottom line and the

erosion of trust by its customers (Hinz et al., 2015). Data breaches due to insecure mobile network infrastructure can be multifaceted. They can be in the form of malware that slows down the network or encrypts mobile devices' hardware until the organization pays a ransom. They can also be malicious software that steals sensitive customer information from databases, and hackers can sell the stolen data on black market sites. The stealing and selling of customer information data on the black market can have a reverberating effect. The stealing and sale of customer data on black markets can also lead to identity theft and undermine an individual's security and privacy. Consequently, mitigating data breaches due to insecure mobile network infrastructure will ensure that customers' data has secure parameters keeping hackers or malicious individuals at bay.

The discoveries from this research study may add to the existing information security awareness and training knowledge base. By presenting strategies from four small to medium organizations, these strategies could be valuable to society by improving how individuals approach and view information and data security. This research study looks at what strategies have been deployed by four different organizations, and which strategies were effective, and which strategies were not effective. Implementing effective strategies through training and awareness on security issues could help mitigate breaches to the mobile network infrastructure and increase overall security compliance. This research could also help raise awareness of the challenges that security managers in developing countries face in catering, creating, and implementing security programs unique to their environment.

Applications to Professional Practice

The specific IT problem that I sought to tackle in this research study was the perceived notion that some security managers lacked strategies to protect mobile network infrastructure from cyberattacks. Furthermore, security managers in developing countries could improve and take advantage of the strategies to mitigate data breaches on mobile network infrastructures by deploying strategies uncovered in this research study. The relative number of the participants interviewed for this research study mentioned that their involvement in this research study has impacted the enhancement of their organization's current strategies. Those participants hope to share what they learned from this research study with other developing countries' security managers.

This research study's discoveries could reduce the number of breaches on mobile network infrastructures. By mitigating the breaches and attacks on the mobile network infrastructure, organizations stand to protect their digital assets and reduce those costs breaches to the organization. Low (2017) argued that the cost of networks and data breaches to small and medium businesses was roughly between $97,000 to $400,000 per year, and between $2 million and $4 million for larger enterprises. Additionally, organizations could face more costs associated with network and data breaches, not to forget the loss of revenues. In the end, the discoveries of this research study could benefit security managers in developing countries. By furnishing the different strategies discovered in this research study, security managers in developing countries will better protect their mobile networks. Security managers in developing countries may utilize the

strategies uncovered in this research study as a blueprint to upgrade and improve their security conceptualization.

Recommendations for Action

This research study's findings may help security managers in developing countries by presenting them with strategies they could utilize to secure their mobile network infrastructures. The first recommendation calls for security managers to look at how they are crafting security training and awareness in their organizations. This research study has revealed that security managers utilize vital strategies to mitigate breaches to the mobile network infrastructure through security awareness and training. Each security managers ought to examine how their organization attains security awareness and training inside the organization. By analyzing this critical area, security managers may uncover areas that need to be fortified better or improved.

The second recommendation request from the study covers infrastructure management tools. Security managers should have a comprehensive review of the infrastructure management tools they are presently using on their mobile network infrastructure. The study will help the security manager determine if the tools they are currently deploying are practical by having an assessment done. Security managers will have the needed information to consider if they should add more infrastructure management tools to supplement what they already have. Each of the participants that took part in this research study agreed about infrastructure management tools. The participants noted that security managers should, at the minimum, have a yearly audit of the infrastructure management tools that their organization is utilizing presently. Having

an audit allocates the security manager and the opportunity to compare and contrast new tools to what they already have. They can decide if they should change, discard, or improve the infrastructure management tools they already have.

The third recommendation request from the study focused on audits. The study findings were that security managers should have an outside firm audit their existing information security strategies. The external audit should establish if they are using the defense-in-depth methodology in the right way. An audit will furnish the security manager with tangible evidence of how their organization utilizes its security setup. Using an outside audit, the security manager will ascertain if they address the organization's critical parts using a layered method. A multi layered security approach is an essential strategy in securing the mobile network infrastructure. Security managers should always know if there are any weaknesses in their mobile networks. Using an outside firm without any bias will help security managers see the shortcomings of their defense-in-depth strategy and shore those weaknesses.

The fourth and final recommendation call centered on the organization's security policies and procedures. Security managers should regularly organize strategic planning meetings with the whole security team and examine their current policies and procedures. Security managers must spearhead the examination of policies and procedures to see if they align with the ones proposed in this research study. Security managers should also network with other security managers in other organizations, which could be advantageous to both enterprises. Additionally, any organization presently operating with no security strategies at all should assess this research study. This study would help them

ascertain if the approach covered in this research study worked for them. By following the four recommendations in this research study, security managers may feel assured that their security methodology will focus on all organizational elements.

Different approaches will be critical to the propagation of the discoveries of this research study. After I have obtained chief academic officer approval, each of the targeted organizations' participants will receive a two-page synopsis of my discoveries. The research study will also be made accessible in the ProQuest database. ProQuest database has active associations with more than 600 colleges and universities globally. Moreover, I intend to pursue publishing my research study in different scholarly journals, publications, and conferences; this will help me reach a wider audience.

Recommendations for Further Study

This research study has unearthed some of the strategies that security managers deploy to protect mobile network infrastructures. Nevertheless, further research on this topic may benefit organizations that have deployed mobile network infrastructure and daily use of those networks. This research study's primary limitation focused on security managers' strategies for small to medium organizations located in Nairobi and Mombasa, Kenya. Recommendations for further research should include similar studies but utilizing different regions in developing countries. I would also recommend a case study that looks at other areas in developing countries to see if they are using the same approach to their mobile network infrastructure security issues.

Furthermore, research performed using a different research design or methodology may also be valuable in the long term. For example, a quantitative research

study is essential in exploring the link between mobile devices' utilization to work and implementing a security framework that the organization must deploy to secure its infrastructure. By having such a study carried out, organizations may see a link between the personal devices and threats to the mobile network infrastructure as the devices log onto the network. In the end, this research study has added to the literature, but further research on the effects of personal mobile devices on the mobile network infrastructure may prove to be beneficial to the information technology industry at large.

Reflections

Undertaking this research study was a challenge, a challenge that I set a goal and decided to wade through the difficulties with the resolve of getting to the other side of the long tunnel. Having a COVID-19 pandemic amid my data collection proved to be another challenge that I had to overcome. However, this study has helped shape my perception of how academic studies are arranged, carried out, and accomplished. The respect that I carry for other individuals and my classmates is immense. In this research study, I focused on making sure that the research study will be credible and use techniques that minimized personal bias from leading me onto the wrong path. As the sole researcher in this study, I was also the primary data collection instrument and reviewed the collected data. I had to keep reminding myself that my personal bias should not sip into the research study.

Additionally, to confirm the research study's credibility, I stringently followed the interview protocols with my participants. I gave each participant a chance to validate my interpretations' exactitude during transcript review and member checking follow-up

sessions with them. Moreover, as the researcher, I ensured that I triangulated the interviews with the collected documents and member checking via transcripts.

A few positive outcomes arose from this research study. The first outcome occurred from the participants' eagerness to interview them and share their knowledge and expertise on the strategies they use to protect mobile network infrastructures. The other outcome rose mainly from my enthusiasm for finishing this research study and my need to explore and share the findings with other researchers. In the end, this research study has encouraged me to start thinking about doing more research studies on different topics that relate to information security.

Summary and Study Conclusions

This multi case qualitative study's main objective was to explore strategies that security managers deploy to secure mobile network infrastructures. The organizations selected for this research study were small to medium businesses in Nairobi and Mombasa, Kenya. The use of methodological triangulation of the collected documents, interviews, transcript reviews, and member checking helped answer the study's core research query. Consequently, four major themes related to security managers' strategies to secure mobile network infrastructures emerged throughout the data evaluation stage. These four major themes, (a) security training and awareness, (b) infrastructure management tools, (c) defense-in-depth, and (d) security governance framework. These major themes helped signal a necessity for security managers to spearhead strategies that revolve around these themes that might help mitigate attacks on mobile network infrastructures. Tchernykh et al. (2019) noted that organizations are always a target of

hackers and a network or data breach may happen any time. By adhering to the strategies laid in this research study, security managers can design strategies that protect mobile networks and plan for the worst-case scenario and prepare for the after-effects of a breach.

References

Adams, C., & Manen, M. A. (2017). Teaching phenomenological research and writing. *Qualitative Health Research, 27*(6), 780-791. https://doi.org/10.1177%2F1049732317698960

Aesaert, K., Voogt, J., Kuiper, E., & Braak, J. V. (2017). Accuracy and bias of ICT self-efficacy: An empirical study into students' over- and underestimation of their ICT competencies. *Computers in Human Behavior*, *75*, 92–102. https://doi.org/10.1016/j.chb.2017.05.010

Ahmed, K., & El-Henawy, I. (2017). Increasing the robustness of data encryption standard by integrating DNA cryptography. *International Journal of Computers and Applications, 39*(2), 91-105. https://doi.org/10.1080/1206212x.2017.1289690

Ajzen, I. (2014). The theory of planned behavior is alive and well, and not ready to retire: A commentary on Sniehotta, Presseau, and Araújo-Soares. *Health Psychology Review, 9*(2), 131-137. https://doi.org/10.1080/17437199.2014.883474

Alase, A. (2017). The interpretative phenomenological analysis (IPA): A guide to a good qualitative research approach. *International Journal of Education and Literacy Studies, 5*(2), 9-17. http://doi.org/10.7575/aiac.ijels.v.5n.2p.9

Aldossary, S., & Allen, W. (2016). Data security, privacy, availability, and integrity in cloud computing: Issues and current solutions. *International Journal of Advanced Computer Science and Applications, 7*(4), 485-498. http://doi.org/10.14569/ijacsa.2016.070464

Ali, S., Green, P., & Robb, A. (2015). Information technology investment governance:

What is it, and does it matter? *International Journal of Accounting Information Systems, 18*, 1-25. https://doi.org/10.1016/j.accinf.2015.04.002

Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building a hybrid efficient model. *Journal of Computational Science, 25*, 152-160. http://doi:10.1016/j.jocs.2017.03.006

Allen, R. E., & Wiles, J. L. (2015). A rose by any other name: Participants choosing research pseudonyms. *Qualitative Research in Psychology, 13*(2), 149-165. https://doi:10.1080/14780887.2015.1133746

Almalki, S. (2016). Integrating quantitative and qualitative data in mixed methods research—Challenges and benefits. *Journal of Education and Learning, 5*(3), 288. https://doi:10.5539/jel.v5n3p288

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). *International Journal of Information Management, 36*(6), 907-916. https://doi:10.1016/j.ijinfomgt.2016.05.017

Al-Rimy, B. A., Maarof, M. A., & Shaid, S. Z. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security, 74*, 144-166. https://doi:10.1016/j.cose.2018.01.001

Al-Safwani, N., Fazea, Y., & Ibrahim, H. (2018). ISCP: In-depth model for selecting

critical security controls. *Computers & Security, 77*, 565-577. http://doi:10.1016/j.cose.2018.05.009

Amin, R., Islam, S. H., Kumar, N., & Choo, K. R. (2018). An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. *Journal of Network and Computer Applications, 104*, 133-144. http://doi:10.1016/j.jnca.2017.12.012

Arsel, Z. (2017). Asking questions with reflexive focus: A tutorial on designing and conducting Interviews. *Journal of Consumer Research, 44*(4), 939–948. https://doi:10.1093/jcr/ucx096

Asimi, Y., Asimi, A., Guezzaz, A., Tbatou, Z., & Sadqi, Y. (2018). Unpredictable cryptographic primitives for the robust wireless network security. *Procedia Computer Science, 134*, 316–321. http://doi:10.1016/j.procs.2018.07.178

Aunger, R., & Curtis, V. (2016). Behavior centered design: Towards an applied science of behavior change. *Health Psychology Review, 10*(4), 425-446. https://doi:10.1080/17437199.2016.1219673

Baker, J. D. (2016). The purpose, process, and methods of writing a literature review. *AORN Journal, 103*(3), 265-269. https://doi:10.1016/j.aorn.2016.01.016

Balmer, D. F., Rama, J. A., Martimianakis, M. A., & Stenfors-Hayes, T. (2016). Using data from program evaluations for qualitative research. *Journal of Graduate Medical Education, 8*(5), 773-774. https://doi:10.4300/jgme-d-16-00540.1

Bandura, A. (1986). The explanatory and predictive scope of self-efficacy theory. *Journal of Social and Clinical Psychology, 4*(3), 359-373.

https://doi:10.1521/jscp.1986.4.3.359

Bandura, A. (1998). Health promotion from the perspective of social cognitive theory. *Psychology & Health, 13*(4), 623-649. https://doi:10.1080/08870449808407422

Bandura, A. (1999). Social cognitive theory: An agentic perspective. *Asian Journal of Social Psychology, 2*(1), 21-41. https://doi:10.1111/1467-839x.00024

Bansal, P., Smith, W. K., & Vaara, E. (2018). New ways of seeing through qualitative research. *Academy of Management Journal, 61*(4), 1189-1195. http://doi:10.5465/amj.2018.4004

Beauchamp, M. R., Crawford, K. L., & Jackson, B. (2019). Social cognitive theory and physical activity: Mechanisms of behavior change, critique, and legacy. *Psychology of Sport and Exercise, 42*, 110-117. https://doi:10.1016/j.psychsport.2018.11.009

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management, 54*(7), 887-901. https://doi:10.1016/j.im.2017.01.003

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cybersecurity knowledge on attack detection. *Computers in Human Behavior, 48*, 51-61. https://doi:10.1016/j.chb.2015.01.039

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open, 2*, 8-14. https://doi:10.1016/j.npls.2016.01.001

Ben-Zeev, D. (2018). Mobile health for mental health in West Africa: The case for

Ghana. *Psychiatric Services*, *69*(7), 741–743. https://doi:10.1176/appi.ps.201700555

Bermejo, P. H., Tonelli, A. O., Zambalde, A. L., Santos, P. A., & Zuppo, L. (2014). Evaluating IT governance practices and business and IT outcomes: A quantitative exploratory study in Brazilian companies. *Procedia Technology, 16,* 849-857. https://doi:10.1016/j.protcy.2014.10.035

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking. *Qualitative Health Research, 26*(13), 1802-1811. https://doi:10.1177/1049732316654870

Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018). Taxonomy of mobile user's security awareness. *Computers & Security, 73,* 266-293. https://doi:10.1016/j.cose.2017.10.015

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviors. *Computers in Human Behavior, 87,* 87-97. https://doi:10.1016/j.chb.2018.05.023

Boateng, H., Adam, D. R., Okoe, A. F., & Anning-Dorson, T. (2016). Assessing the determinants of internet banking adoption intentions: A social cognitive theory perspective. *Computers in Human Behavior, 65,* 468-478. https://doi:10.1016/j.chb.2016.09.017

Brown, J. B., Ryan, B. L., Thorpe, C., Markle, E. K., Hutchison, B., & Glazier, R. H. (2015). Measuring teamwork in primary care: Triangulation of qualitative and quantitative data. *Families, Systems, & Health, 33*(3), 193-202.

https://doi:10.1037/fsh0000109

Bugliesi, M., Calzavara, S., & Focardi, R. (2017). Formal methods for web security. *Journal of Logical and Algebraic Methods in Programming, 87*, 110-126. https://doi:10.1016/j.jlamp.2016.08.006

Burney, V. H. (2008). Applications of social cognitive theory to gifted education. *Roeper Review*, *30*(2), 130–139. https://doi:10.1080/02783190801955335

Bush, A. A., & Amechi, M. H. (2019). Conducting and presenting qualitative research in pharmacy education. *Currents in Pharmacy Teaching and Learning*, *11*(6), 638–650. https://doi:10.1016/j.cptl.2019.02.030

Cajka, J., Amer, S., Ridenhour, J., & Allpress, J. (2018). Geo-sampling in developing nations. *International Journal of Social Research Methodology*, *21*(6), 729–746. http://doi:10.1080/13645579.2018.1484989

Carter, J. G., Piza, E. L., & Grommon, E. (2018). Leveraging wireless broadband to improve police land mobile radio programming: Estimating the resource impact. *Journal of Crime and Justice, 42*(1), 60-77. http://doi:10.1080/0735648x.2018.1554844

Carvalho, M. B., Bellotti, F., Berta, R., Gloria, A. D., & Sedano, C. (2015). An activity theory-based model for serious games analysis and conceptual design. *Computers & Education, 87,* 166-181. http://doi:10.1016/j.compedu.2015.03.023

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report, 21(5),* 811-831. https://nsuworks.nova.edu/tqr/vol21/iss5/2

Catalano, H. P., Knowlden, A. P., Sharma, M., & Franzidis, A. (2016). A pilot study in applying social cognitive theory to predict HPV vaccination intentions of unvaccinated college women. *American Journal of Sexuality Education, 11*(4), 287-305. https://doi:10.1080/15546128.2016.1231648

Chapman, A., Hadfield, M., & Chapman, C. (2015). Qualitative research in healthcare: An introduction to grounded theory using thematic analysis. *Journal of the Royal College of Physicians of Edinburgh*, *45*(3), 201–205. https://doi:10.4997/jrcpe.2015.305

Chen, X., Chen, L., & Wu, D. (2016). Factors that influence employees' security policy Compliance: An awareness-motivation-capability perspective. *Journal of Computer Information Systems*, *58*(4), 312-324. https://doi:10.1080/08874417.2016.1258679

Chen, Y., Ramamurthy, K. R., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11–19. http://doi:10.1080/08874417.2015.11645767

Chowdhury, M. F. (2014). Coding, sorting and sifting of qualitative data analysis: Debates and discussion. *Quality & Quantity*, *49*(3), 1135-1143. http://doi:10.1007/s11135-014-0039-2

Clarke, R., & Wigan, M. (2018). The information infrastructures of 1985 and 2018: The sociotechnical context of computer law & security. *Computer Law & Security Review, 34*(4), 677-700. https://doi:10.1016/j.clsr.2018.05.006

Colombo, P., & Ferrari, E. (2015). Privacy-aware access control for big data: A research roadmap. *Big Data Research, 2*(4), 145-154. https://doi:10.1016/j.bdr.2015.08.001

Colorafi, K. J., & Evans, B. (2016). Qualitative descriptive methods in health science research. *HERD: Health Environments Research & Design Journal, 9*(4), 16-25. http://doi:10.1177/1937586715614171

Constantinou, C. S., Georgiou, M., & Perdikogianni, M. (2017). A comparative method for themes saturation (CoMeTS) in qualitative interviews. *Qualitative Research, 17*(5), 571-588. https://doi:10.1177/1468794116686650

Cook, D. A., Kuper, A., Hatala, R., & Ginsburg, S. (2016). When assessment data are words. *Academic Medicine, 91*(10), 1359-1369. https://doi:10.1097/acm.0000000000001175

Crane, S., & Broome, M. E. (2017). Understanding ethical issues of research participation from the perspective of participating children and adolescents: A systematic review. *Worldviews on Evidence-Based Nursing, 14*(3), 200-209. https://doi:10.1111/wvn.12209

Creech, G., & Hu, J. (2014). A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns. *IEEE Transactions on Computers, 63*(4), 807-819. http://doi:10.1109/tc.2013.13

Crowther, S., Ironside, P., Spence, D., & Smythe, L. (2016). Crafting stories in hermeneutic phenomenology research: A methodological device. *Qualitative Health Research, 27*(6), 826-835. https://doi:10.1177/1049732316656161

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research. *Dimensions of Critical Care Nursing, 36*(4), 253-263. http://doi:10.1097/dcc.0000000000000253

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information and Computer Security, 24*(1), 116-134. https://doi:10.1108/ics-04-2015-0018

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982-1003. https://pubsonline.informs.org/doi/abs/10.1287/mnsc.35.8.982

Dempsey, L., Dowling, M., Larkin, P., & Murphy, K. (2016). Sensitive interviewing in qualitative research. *Research in Nursing & Health, 39*(6), 480-490. https://doi:10.1002/nur.21743

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic Insurance). *The Qualitative Report*, *21*(3), 521-528. https://nsuworks.nova.edu/tqr/vol21/iss3/6 doi:10.7748/nr.22.4.8.e1317

Dye, S. M., & Scarfone, K. (2014). A standard for developing secure mobile applications. *Computer Standards & Interfaces*, *36*(3), 524–530. https://doi:10.1016/j.csi.2013.09.005

Ellinger, A. D., & Mcwhorter, R. (2016). Qualitative case study research as empirical inquiry. *International Journal of Adult Vocational Education and Technology*, *7*(3), 1–13. https://doi:10.4018/ijavet.2016070101

Elsayed, M., & Zulkernine, M. (2019). Offering security diagnosis as a service for cloud

SaaS applications. *Journal of Information Security and Applications, 44*, 32-48. https://doi:10.1016/j.jisa.2018.11.006

Elst, T. V., Broeck, A. V., Cuyper, N. D., & Witte, H. D. (2014). On the reciprocal relationship between job insecurity and employee well-being: Mediation by perceived control? *Journal of Occupational and Organizational Psychology, 87*(4), 671-693. https://doi:10.1111/joop.12068

Erlingsson, C., & Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African Journal of Emergency Medicine*, *7*(3), 93–99. https://doi:10.1016/j.afjem.2017.08.001

Etaiwi, W. A., & Hraiz, S. (2018). Structured encryption algorithm for text cryptography. *Journal of Discrete Mathematical Sciences and Cryptography, 21*(7-8), 1559-1572. https://doi:10.1080/09720529.2018.1516723

Fatima, K., Ahmed, Z., & Fatima, A. (2017). Jackknife replication variance estimation of population total under systematic sampling with varying probabilities. *Matrix Science Mathematics*, *1*(1), 34–39. https://doi:10.26480/msmk.01.2017.34.39

Fenny, A. P., Kusi, A., Arhinful, D. K., & Asante, F. A. (2016). Factors contributing to low uptake and renewal of health insurance: A qualitative study in Ghana. *Global Health Research and Policy, 1*(1). https://doi:10.1186/s41256-016-0018-3

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how, and who. *Computers & Security, 61*, 169-183. https://doi:10.1016/j.cose.2016.06.002

Fuchs, M., & Schalljo, M. (2017). Global encounters challenge Western rationality

assumptions. *Science as Culture, 26*(4), 520-528. https://doi:10.1080/09505431.2017.1354845

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change, 10*(1), 19-32. https://doi:10.5590/JOSC.2018.10.1.02

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, 20(9), 1408-1416. http://nsuworks.nova.edu/tqr/vol20/iss9/3

Gainotti, S., Turner, C., Woods, S., Kole, A., Mccormack, P., Lochmüller, H., & Mascalzoni, D. 2016). Improving the informed consent process in international collaborative rare disease research: Effective consent for effective research. *European Journal of Human Genetics, 24*(9), 1248-1254. http://doi:10.1038/ejhg.2016.2

Gao, Y., Ao, H., Feng, Z., Zhou, W., Hu, S., & Tang, W. (2018). Mobile network security and privacy in WSN. *Procedia Computer Science, 129*, 324-330. http://doi:10.1016/j.procs.2018.03.083

Garavan, T., Mccarthy, A., Sheehan, M., Lai, Y., Saunders, M. N. K., Clarke, N., & Shanahan, V. (2019). Measuring the organizational impact of training: The need for greater methodological rigor. *Human Resource Development Quarterly*, *30*(3), 291–309. https://doi:10.1002/hrdq.21345

Garg, N., & Bawa, S. (2016). Comparative analysis of cloud data integrity auditing protocols. *Journal of Network and Computer Applications, 66*, 17-32.

https://doi:10.1016/j.jnca.2016.03.010

Gedera, D. S. (2016). The application of activity theory in identifying contradictions in a university blended learning course. *Activity Theory in Education,* 53-69. http://doi:10.1007/978-94-6300-387-2_4

Gehman, J., Glaser, V. L., Eisenhardt, K. M., Gioia, D., Langley, A., & Corley, K. G. (2017). Finding theory–method fit: A comparison of three qualitative approaches to theory building. *Journal of Management Inquiry*, *27*(3), 284-300. http://doi:10.1177/1056492617706029

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report, 20*(11), 1772-1789. https://nsuworks.nova.edu/tqr/vol20/iss11/5

Ghanbari, Z., Rahmani, Y., Ghaffarian, H., & Ahmadzadegan, M. H. (2015). Comparative approach to web application firewalls. *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, *3*(1), 115–145. https://doi:10.1109/kbei.2015.7436148

Gist, M. E., Schwoerer, C., & Rosen, B. (1989). Effects of alternative training methods on self-efficacy and performance in computer software training. *Journal of Applied Psychology, 74*(6), 884-891. https://doi:10.1037//0021-9010.74.6.884

Gokhale, A. S., & Waghmare, V. S. (2016). The shoulder surfing resistant graphical password authentication technique. *Procedia Computer Science, 79,* 875-884. https://doi:10.1016/j.procs.2016.03.091

Gommans, L., Vollbrecht, J., Bruijn, B. G., & Laat, C. D. (2015). The service provider

group framework. *Future Generation Computer Systems, 45*, 176-192. https://doi:10.1016/j.future.2014.06.002

Graneheim, U. H., Lindgren, B.-M., & Lundman, B. (2017). Methodological challenges in qualitative content analysis: A discussion paper. *Nurse Education Today*, *56*, 29–34. https://doi:10.1016/j.nedt.2017.06.002

Gunawan, J. (2015). Ensuring trustworthiness in qualitative research. *Belitung Nursing Journal*, *1*(1), 10-11. https://doi:10.33546/bnj.4

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2016). Fighting against phishing attacks: State of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629-3654. https://doi:10.1007/s00521-016-2275-y

Hadi, M. A., & Closs, S. J. (2015). Ensuring rigour and trustworthiness of qualitative research in clinical pharmacy. *International Journal of Clinical Pharmacy*, *38*(3), 641–646. https://doi:10.1007/s11096-015-0237-6

Hannon, B., Swami, N., Rodin, G., Pope, A., & Zimmermann, C. (2016). Experiences of patients and caregivers with early palliative care: A qualitative study. *Palliative Medicine*, *31*(1), 72–81. https://doi:10.1177/0269216316649126

Hanus, B., & Wu, Y. (2015). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16. https://doi:10.1080/10580530.2015.1117842

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*(2), 172-183.

https://doi:10.1002/jcad.12074

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, *18*(2), 106-125. https://doi:10.1057/ejis.2009.6

Hert, P. D., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, *32*(2), 179–194. https://doi:10.1016/j.clsr.2016.02.006

Hilia, M., Chibani, A., Winter, T., & Djouani, K. (2017). Semantic-based authorization framework for multi-domain collaborative cloud environments. *Procedia Computer Science*, *109*, 718-724. https://doi:10.1016/j.procs.2017.05.427

Hina, S., & Dominic, P. D. (2018). Information security policies' compliance: A perspective for higher education institutions. *Journal of Computer Information Systems*, *9*(3), 1-11. https://doi:10.1080/08874417.2018.1432996

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, *52*(3), 337-347. https://doi:10.1016/j.im.2014.12.006

Holen, J. B., Hung, W., & Gourneau, B. (2017). Does one-to-one technology really work: An evaluation through the lens of activity theory. *Computers in the Schools*, *34*(1-2), 24-44. https://doi:10.1080/07380569.2017.1281698

Honicke, T., & Broadbent, J. (2016). The influence of academic self-efficacy on academic performance: A systematic review. *Educational Research Review*, *17*, 63-84. https://doi:10.1016/j.edurev.2015.11.002

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

Høyland, S., Hollund, J. G., & Olsen, O. E. (2015). Gaining access to a research site and participants in medical and nursing research: A synthesis of accounts. *Medical Education*, *49*(2), 224–232. https://doi:10.1111/medu.12622

Huang, C. (2016). Achievement goals and self-efficacy: A meta-analysis. *Educational Research Review*, *19*, 119–137. https://doi:10.1016/j.edurev.2016.07.002

Iacono, V. L., Symonds, P., & Brown, D. H. (2016). Skype as a tool for qualitative research interviews. *Sociological Research Online, 21*(2), 1-15. https://doi:10.5153/sro.3952

Jabez, J., & Muthukumar, B. (2015). Intrusion detection system (IDS): Anomaly detection using outlier detection approach. *Procedia Computer Science, 48*, 338-346. https://doi:10.1016/j.procs.2015.04.191

Jagoda, K., & Samaranayake, P. (2017). An integrated framework for ERP system implementation. *International Journal of Accounting & Information Management, 25*(1), 91-109. https://doi:10.1108/ijaim-04-2016-0038

Jander, K., Braubach, L., & Pokahr, A. (2018). Defense-in-depth and role authentication for microservice systems. *Procedia Computer Science, 130*, 456-463. https://doi:10.1016/j.procs.2018.04.047

Jang, J., Kang, H., Woo, J., Mohaisen, A., & Kim, H. K. (2015). Andro-autopsy: Anti-malware system based on similarity matching of malware and malware creator-

centric information. *Digital Investigation, 14*, 17-35. https://doi:10.1016/j.diin.2015.06.002

Jenkins, S. A. (2015). Assistants, guides, collaborators, friends: The concealed figures of conflict research. *Journal of Contemporary Ethnography*, *47*(2), 143-170. https://doi:10.1177/0891241615619993

Jentoft, N., & Olsen, T. S. (2017). Against the flow in data collection: How data triangulation combined with a 'slow' interview technique enriches data. *Qualitative Social Work, 18*(2), 179-193. https://doi:10.1177/1473325017712581

Jingyao, S., Chandel, S., Yunnan, Y., Jingji, Z., & Zhipeng, Z. (2019). Securing a network: How effective using firewalls and VPNs are? *Advances in Biochemical Engineering/Biotechnology, 21*(5), 1050-1068. https://doi:10.1007/978-3-030-12385-7_71

Joshi, A., Bollen, L., Hassink, H., Haes, S. D., & Grembergen, W. V. (2018). Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. *Information & Management, 55*(3), 368-380. https://doi:10.1016/j.im.2017.09.003

Kallio, H., Pietilä, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing, 72*(12), 2954-2965. https://doi:10.1111/jan.13031

Kaptelinin, V., & Nardi, B. (2017). Activity theory as a framework for human-technology

interaction research. *Mind, Culture, and Activity, 25*(1), 3-5. https://doi:10.1080/10749039.2017.1393089

Kelly, P., Fitzsimons, C., & Baker, G. (2016). Should we reframe how we think about physical activity and sedentary behaviour measurement? Validity and reliability reconsidered. *International Journal of Behavioral Nutrition and Physical Activity, 13*(1), 32–45. https://doi:10.1186/s12966-016-0351-4

Khoumsi, A., Erradi, M., & Krombi, W. (2018). A formal basis for the design and analysis of firewall security policies. *Journal of King Saud University - Computer and Information Sciences, 30*(1), 51-66. https://doi:10.1016/j.jksuci.2016.11.008

Kim, B., & Park, M. J. (2017). Effect of personal factors to use ICTs on e-learning adoption: Comparison between learner and instructor in developing countries. *Information Technology for Development, 24*(4), 706-732. https://doi:10.1080/02681102.2017.1312244

Korpela, M., Mursu, A., Soriyan, A., Eerola, A., Häkkinen, H., & Toivanen, M. (2007). Information systems research and development by activity analysis and development: Dead horse or the next wave? *Information Systems Research IFIP International Federation for Information Processing, 10*(2), 453-471. https://doi:10.1007/1-4020-8095-6_25

Kos, A., Milutinović, V., & Umek, A. (2019). Challenges in wireless communication for connected sensors and wearable devices used in sport biofeedback applications. *Future Generation Computer Systems, 92*, 582-592. https://doi:10.1016/j.future.2018.03.032

Kozleski, E. B. (2017). The uses of qualitative research. *Research and practice for persons with severe disabilities, 42*(1), 19-32. https://doi:10.1177/1540796916683710

Kroeger, C. M., Garza, C., Lynch, C. J., Myers, E., Rowe, S., Schneeman, B. O., & Allison, D. B. (2018). Scientific rigor and credibility in the nutrition research landscape. *The American Journal of Clinical Nutrition, 107*(3), 484-494. https://doi:10.1093/ajcn/nqx067

Lancaster, K. (2016). Confidentiality, anonymity, and power relations in elite interviewing: Conducting qualitative policy research in a politicized domain. *International Journal of Social Research Methodology, 20*(1), 93-103. https://doi:10.1080/13645579.2015.1123555

Lapkin, S., Levett-Jones, T., & Gilligan, C. (2015). Using the theory of planned behavior to examine health professional students' behavioral intentions in relation to medication safety and collaborative practice. *Nurse Education Today, 35*(8), 935-940. https://doi:10.1016/j.nedt.2015.03.018

Lazzez, A., & Slimani, T. (2015). Forensics investigation of web application security attacks. *International Journal of Computer Network and Information Security, 7* (3), 10–17. https://doi:10.5815/ijcnis.2015.03.02

Le, V. H., Hartog, J. D., & Zannone, N. (2018). Security and privacy for innovative automotive applications: A survey. *Computer Communications, 132*, 17-41. https://doi:10.1016/j.comcom.2018.09.010

Learmonth, Y. C., Adamson, B. C., Balto, J. M., Chiu, C.-Y., Molina-Guzman, I.,

Finlayson, M., & Motl, R. W. (2016). Multiple sclerosis patients need and want information on exercise promotion from healthcare providers: A qualitative study. *Health Expectations*, *20*(4), 574–583. https://doi:10.1111/hex.12482

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049-1092. https://doi:10.1108/mrr-04-2013-0085

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324. https://doi:10.4103/2249-4863.161306

Levitt, H. M., Motulsky, S. L., Wertz, F. J., Morrow, S. L., & Ponterotto, J. G. (2017). Recommendations for designing and reviewing qualitative research in psychology: Promoting methodological integrity. *Qualitative Psychology*, *4*(1), 2–22. https://doi:10.1037/qup0000082

Li, R., Asaeda, H., Li, J., & Fu, X. (2017). A distributed authentication and authorization scheme for in-network big data sharing. *Digital Communications and Networks*, *3*(4), 226-235. https://doi:10.1016/j.dcan.2017.06.001

Li, X., Xiang, T., Chen, F., & Guo, S. (2018). Efficient biometric identity-based encryption. *Information Sciences*, *465*, 248-264. https://doi:10.1016/j.ins.2018.07.028

Lin, H., & Chang, C. (2018). What motivates health information exchange in social media? The roles of the social cognitive theory and perceived interactivity. *Information & Management*, *55*(6), 771-780.

https://doi:10.1016/j.im.2018.03.006

Lishner, D. A. (2015). A concise set of core recommendations to improve the dependability of psychological research. *Review of General Psychology, 19*(1), 52-68. https://doi:10.1037/gpr0000028

Lo, N., Wu, C., & Chuang, Y. (2017). An authentication and authorization mechanism for long-term electronic health records management. *Procedia Computer Science, 111*, 145-153. https://doi:10.1016/j.procs.2017.06.021

Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud & Security, 2017*(4), 18-20. https://doi:10.1016/s1361-3723(17)30034-9

Lynch, S. E., & Mors, M. L. (2019). Strategy implementation and organizational change: How formal reorganization affects professional networks. *Long Range Planning, 52*(2), 255-270. https://doi:10.1016/j.lrp.2018.02.003

Madlock, P. E. (2018). Managing the implementation of new computer systems in small businesses: Building attitudes and perceptions. *American Journal of Management, 18*(2), 56-69. https://articlegateway.com/index.php/AJM/article/view/293

Maher, C., Hadfield, M., Hutchings, M., & Eyto, A. D. (2018). Ensuring rigor in qualitative data analysis. *International Journal of Qualitative Methods, 17*(1), 112-121. https://doi:10.1177/1609406918786362

Mahmud, M. T., Rahman, M. O., Hassan, M. M., Almogren, A., & Zhou, M. (2019). An Efficient cooperative medium access control protocol for wireless IoT networks in the smart world system. *Journal of Network and Computer Applications, 133*, 26–

38. https://doi:10.1016/j.jnca.2019.02.011

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior, 83*, 32-44. https://doi:10.1016/j.chb.2018.01.028

Manning, J. M. (2017). Does the law on compensation for research-related injury in the UK, Australia, and New Zealand meet ethical requirements? *Medical Law Review, 25*(3), 397-427. https://doi:10.1093/medlaw/fwx019

Manser, K., Hillebrand, B., Woolthuis, R. K., Ziggers, G. W., Driessen, P. H., & Bloemer, J. (2016). An activities-based approach to network management: An explorative study. *Industrial Marketing Management, 55*, 187-199. https://doi:10.1016/j.indmarman.2015.10.004

Marshall, I., & Wallace, B. C. (2019). Toward systematic review automation: a practical guide to using machine learning tools in research synthesis. Systematic Reviews, 8(1). https://doi.org/10.1186/s13643-019-1074-9

Masta, S., & Rosa, T. J. (2019). Understanding the dominant discourse of colonialism: A qualitative, single case study of an eighth-grade U.S. history classroom. *The Social Studies, 110*(3), 146-154. https://doi:10.1080/00377996.2019.1585317

Mccusker, K., & Gunaydin, S. (2014). Research using qualitative, quantitative, or mixed methods and choices based on the research. *Perfusion, 30*(7), 537-542. https://doi:10.1177/0267659114559116

Mcdermid, F., Peters, K., Daly, J., & Jackson, D. (2016). Developing resilience: Stories from novice nurse academics. *Nurse Education Today, 38*, 29-35.

https://doi:10.1016/j.nedt.2016.01.002

Mcdonald, K. E., Conroy, N. E., Kim, C. I., Lobraico, E. J., Prather, E. M., & Olick, R. S. (2016). Is safety in the eye of the beholder? Safeguards in research with adults with intellectual disability. *Journal of Empirical Research on Human Research Ethics, 11*(5), 424-438. https://doi:10.1177/1556264616651182

Mcintosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research*, *2*(1), 23–33. https://doi:10.1177/2333393615597674

Mckim, C. A. (2016). The value of mixed methods research. *Journal of Mixed Methods Research, 11*(2), 202-222. https://doi:10.1177/1558689815607096

Mishra, D., Das, A. K., Chaturvedi, A., & Mukhopadhyay, S. (2015). A secure password-based authentication and key agreement scheme using smart cards. *Journal of Information Security and Applications, 23*, 28-43. https://doi:10.1016/j.jisa.2015.06.003

Moghadam, R. S., & Colomo-Palacios, R. (2018). Information security governance in big data environments: A systematic mapping. *Procedia Computer Science*, *138*, 401-408. https://doi:10.1016/j.procs.2018.10.057

Morato, D., Berrueta, E., Magaña, E., & Izal, M. (2018). Ransomware early detection by the analysis of file-sharing traffic. *Journal of Network and Computer Applications, 124*, 14-32. https://doi:10.1016/j.jnca.2018.09.013

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research, 25*(9), 1212-1222.

https://doi:10.1177/1049732315588501

Moser, A., & Korstjens, I. (2017). Practical guidance to qualitative research. Part 3: Sampling, data collection, and analysis. *European Journal of General Practice*, *24*(1), 9–18. https://doi:10.1080/13814788.2017.1375091

Mullan, B., Allom, V., Sainsbury, K., & Monds, L. A. (2015). Examining the predictive utility of an extended theory of planned behavior model in the context of specific individual safe food-handling. *Appetite, 90*, 91-98. https://doi:10.1016/j.appet.2015.02.033

Nassaji, H. (2015). Qualitative and descriptive research: Data type versus data analysis. *Language Teaching Research, 19*(2), 129-132. https://doi:10.1177/1362168815572747

Nejat, S. K., & Kabiri, P. (2017). An adaptive and cost-based intrusion response system. *Cybernetics and Systems, 48*(6-7), 495-509. https://doi:10.1080/01969722.2017.1319693

Ng, B., Kankanhalli, A., & Xu, Y. (2009). Studying user's computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825. https://doi:10.1016/j.dss.2008.11.010

Ng, T. W. H., & Lucianetti, L. (2016). Within-individual increases in innovative behavior and creative, persuasion, and change self-efficacy over time: A social–cognitive theory perspective. *Journal of Applied Psychology*, *101*(1), 14–34. https://doi:10.1037/apl0000029

Nivethan, J., & Papa, M. (2016). On the use of open-source firewalls in ICS/SCADA

systems. *Information Security Journal: A Global Perspective, 25*(1-3), 83-93. https://doi:10.1080/19393555.2016.1172283

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis. *International Journal of Qualitative Methods*, *16*(1), 160940691773384. https://doi:10.1177/1609406917733847

Ochang, P. A., Irving, P. J., & Ofem, P. O. (2016). Research on wireless network security awareness of average users. *International Journal of Wireless and Microwave Technologies*, *6*(2), 21–29. https://doi:10.5815/ijwmt.2016.02.03

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity strategy's role in raising Kenyan awareness of mobile security threats. *Information & Security*, *32*(2), 1-20. https://doi:10.11610/isij.3207

Oreilly, C. M., Gougis, R. D., Klug, J. L., Carey, C. C., Richardson, D. C., Bader, N. E., & Hunter, W. (2017). Using large data sets for open-ended inquiry in undergraduate science classrooms. *BioScience*, *67*(12), 1052-1061. https://doi:10.1093/biosci/bix118

Ozyilmaz, A., Erdogan, B., & Karaeminogullari, A. (2017). Trust in the organization as a moderator of the relationship between self-efficacy and workplace outcomes: A social cognitive theory-based examination. *Journal of Occupational and Organizational Psychology*, *91*(1), 181-204. https://doi:10.1111/joop.12189

Panadero, E., Jonsson, A., & Botella, J. (2017). Effects of self-assessment on self-regulated learning and self-efficacy: Four meta-analyses. *Educational Research Review*, *22*, 74-98. https://doi:10.1016/j.edurev.2017.08.004

Peng, J., Choo, K. R., & Ashman, H. (2016). User profiling in intrusion detection: A review. *Journal of Network and Computer Applications, 72*, 14-27. https://doi:10.1016/j.jnca.2016.06.012

Percy, W. H., Kostere, K., & Kostere, S. (2015). Generic qualitative research in psychology. *The Qualitative Report, 20*(2), 76-85. Retrieved from https://nsuworks.nova.edu/tqr/vol20/iss2/7

Potey, M. M., Dhote, C., & Sharma, D. H. (2016). Homomorphic encryption for the security of cloud data. *Procedia Computer Science, 79*, 175-181. https://doi:10.1016/j.procs.2016.03.023

Poullet, Y. (2018). Is the general data protection regulation the solution? *Computer Law & Security Review, 34*(4), 773-778. https://doi:10.1016/j.clsr.2018.05.021

Rana, N. P., & Dwivedi, Y. K. (2015). Citizens adoption of an e-government system: Validating extended social cognitive theory (SCT). *Government Information Quarterly, 32*(2), 172-181. https://doi:10.1016/j.giq.2015.02.002

Rashid, M., Caine, V., & Goez, H. (2015). The encounters and challenges of ethnography as a methodology in health research. *International Journal of Qualitative Methods, 14*(5), 16-29. https://doi:10.1177/1609406915621421

Raterink, G. (2016). Reflective journaling for critical thinking development in advanced practice registered nurse students. *Journal of Nursing Education, 55*(2), 101-104. https://doi:10.3928/01484834-20160114-08

Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). A secure communicating things network framework for Industrial IoT using blockchain technology. *Ad Hoc*

Networks, 94, 101-133. https://doi:10.1016/j.adhoc.2019.101933

Rawal, B. S. (2018). Proxy re-encryption architect for storing and sharing of cloud contents. *International Journal of Parallel, Emergent, and Distributed Systems, 4*(2), 1-17. https://doi:10.1080/17445760.2018.1439491

Razzaq, A., Anwar, Z., Ahmad, H. F., Latif, K., & Munir, F. (2014). Ontology for attack detection: An intelligent approach to web application security. *Computers & Security, 45*, 124-146. https://doi:10.1016/j.cose.2014.05.005

Reinecke, J., Arnold, D. G., & Palazzo, G. (2016). Qualitative methods in business ethics, corporate responsibility, and sustainability research. *Business Ethics Quarterly, 26*(4), xiii-xxii. https://doi:10.1017/beq.2016.67

Rhee, H., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end-users' information security practice behavior. *Computers & Security, 28*(8), 816-826. https://doi:10.1016/j.cose.2009.05.008

Roozbahani, F. S., & Azad, R. (2015). Security solutions against computer network threats. *International Journal of Advanced Networking and Applications, 7*(1), 2576-2581. https://www.ijana.in/papers/V7I-1.pdf

Rosenthal, M. (2016). Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in Pharmacy Teaching and Learning, 8*(4), 509-516. https://doi:10.1016/j.cptl.2016.03.021

Roulston, K. (2016). Issues involved in methodological analyses of research interviews. *Qualitative Research Journal, 16*(1), 68–79. http://doi:10.1108/qrj-02-2015-0015

Roux, C. S. (2016). Exploring rigour in autoethnographic research. *International Journal of Social Research Methodology, 20*(2), 195-207. https://doi:10.1080/13645579.2016.1140965

Rubenstein, L. D., Ridgley, L. M., Callan, G. L., Karami, S., & Ehlinger, J. (2018). How teachers perceive factors that influence creativity development: Applying a social cognitive theory perspective. *Teaching and Teacher Education, 70*, 100-110. https://doi:10.1016/j.tate.2017.11.012

Salah, K., Calyam, P., & Boutaba, R. (2017). Analytical model for elastic scaling of cloud-based firewalls. *IEEE Transactions on Network and Service Management, 14*(1), 136-146. https://doi:10.1109/tnsm.2016.2640297

Sarika, S., Pravin, A., Vijayakumar, A., & Selvamani, K. (2016). Security issues in mobile ad hoc networks. *Procedia Computer Science, 92*, 329-335. https://doi:10.1016/j.procs.2016.07.363

Sarma, S. K. (2015). Qualitative research: Examining the misconceptions. *South Asian Journal of Management, 22*(3), 176-191. Retrieved from http://www.questia.com/library/journal/1P3-3861238831

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., & Jinks, C. (2017). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893–1907. https://doi:10.1007/s11135-017-0574-8

Saxena, S., & Agarwal, D. (2018). Confidentiality assessment model to estimate security during an effective e-procurement process. *International Journal of Computer*

Sciences and Engineering, 6(1), 361-365. https://doi:10.26438/ijcse/v6i1.361365

Schoenfeld, J., Segal, G., & Borgia, D. (2017). Social cognitive career theory and the goal of becoming a certified public accountant. *Accounting Education, 26*(2), 109-126. https://doi:10.1080/09639284.2016.1274909

Sen, R., & Borle, S. (2015). Estimating the contextual risk of a data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314-341. https://doi:10.1080/07421222.2015.1063315

Sengupta, S. (2016). Admissibility of a variance estimator in finite population sampling under Warner's randomized response plan with multiple responses. *Communications in Statistics - Theory and Methods, 45*(19), 5745-5750. https://doi:10.1080/03610926.2014.948208

Shaw, D., & Satalkar, P. (2018). Researchers' interpretations of research integrity: A qualitative study. *Accountability in Research, 25*(2), 79-93. https://doi:10.1080/08989621.2017.1413940

Sheeran, P., Maki, A., Montanaro, E., Avishai-Yitshak, A., Bryan, A., Klein, W. M., & Rothman, A. J. (2016). The impact of changing attitudes, norms, and self-efficacy on health-related intentions and behavior: A meta-analysis. *Health Psychology, 35*(11), 1178-1188. https://doi:10.1037/hea0000387

Shoji, K., Cieslak, R., Smoktunowicz, E., Rogala, A., Benight, C. C., & Luszczynska, A. (2015). Associations between job burnout and self-efficacy: A meta-analysis. *Anxiety, Stress, & Coping, 29*(4), 367-386. https://doi:10.1080/10615806.2015.1058369

Siciliano, M. D. (2016). It's the quality, not the quantity of ties that matters. *American Educational Research Journal, 53*(2), 227–262. https://doi:10.3102/0002831216629207

Sim, J., Saunders, B., Waterfield, J., & Kingstone, T. (2018). Can sample size in qualitative research be determined a priori? *International Journal of Social Research Methodology, 21*(5), 619–634. https://doi:10.1080/13645579.2018.1454643

Singh, R., Kumar, H., & Singla, R. (2015). An intrusion detection system using network traffic profiling and online sequential extreme learning machine. *Expert Systems with Applications, 42*(22), 8609-8624. https://doi:10.1016/j.eswa.2015.07.015

Smith, A. J., Felix, E. D., Benight, C. C., & Jones, R. T. (2017). Protective factors, coping appraisals, and social barriers predict mental health following community violence: A prospective test of social cognitive theory. *Journal of Traumatic Stress, 30*(3), 245-253. https://doi:10.1002/jts.22197

Smith, B., & Mcgannon, K. R. (2017). 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://doi:10.1080/1750984x.2017.1317357

Söderholm, P., Hellsmark, H., Frishammar, J., Hansson, J., Mossberg, J., & Sandström, A. (2019). Technological development for sustainability: The role of network management in the innovation policy mix. *Technological Forecasting and Social Change, 138*, 309-323. http://doi:10.1016/j.techfore.2018.10.010

Sohn, B. K., Thomas, S. P., Greenberg, K. H., & Pollio, H. R. (2017). Hearing the voices of students and teachers: A phenomenological approach to educational research. *Qualitative Research in Education, 6*(2), 121. http://doi:10.17583/qre.2017.2374

Sommestad, T. (2018). Work-related groups and information security policy compliance. *Information and Computer Security*, *26*(5), 533–550. http://doi:10.1108/ics-08-2017-0054

Sörqvist, P. (2016). Grand challenges in environmental psychology. *Frontiers in Psychology, 7,* 10-15. https://doi:10.3389/fpsyg.2016.00583

Sorsa, M. A., Kiikkala, I., & Åstedt-Kurki, P. (2015). Bracketing as a skill in conducting unstructured qualitative interviews. *Nurse Researcher*, *22*(4), 8–12. https://doi:10.7748/nr.22.4.8.e1317

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cybersecurity: Framework, standards, and recommendations. *Future Generation Computer Systems, 92*, 178-188. https://doi:10.1016/j.future.2018.09.063

Stake, R. (1995). *The art of case study research* (pp. 49-68). Sage.

Stallings, W. (2016). Format-preserving encryption: Overview and NIST specification. *Cryptologia, 41*(2), 137-152. https://doi:10.1080/01611194.2016.1169457

Strickland, J. C., & Stoops, W. W. (2015). Perceptions of research risk and undue influence: Implications for ethics of research conducted with cocaine users. *Drug and Alcohol Dependence, 156*, 304-310.

https://doi:10.1016/j.drugalcdep.2015.09.029

Stuckey, H. (2015). The second step in data analysis: Coding qualitative research data. *Journal of Social Health and Diabetes, 3*(1), 007-010. https://doi:10.4103/2321-0656.140875

Tan, C. B., Hijazi, M. H., Lim, Y., & Gani, A. (2018). A survey on proof of retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions, and future trends. *Journal of Network and Computer Applications, 110*, 75-86. https://doi:10.1016/j.jnca.2018.03.017

Tanaka, Y., Akiyama, M., & Goto, A. (2017). Analysis of malware download sites by focusing on time-series variation of malware. *Journal of Computational Science, 22*, 301-313. https://doi:10.1016/j.jocs.2017.05.027

Tchernykh, A., Schwiegelsohn, U., Talbi, E.-G., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*(1), 100–151. https://doi:10.1016/j.jocs.2016.11.011

Thissen, M. R., & Mason, K. M. (2019). Planning security architecture for health survey data storage and access. *Health Systems, 2*(1), 1-7. https://doi:10.1080/20476965.2019.1599702

Thomann, E., & Maggetti, M. (2017). Designing research with qualitative comparative analysis (QCA) *Sociological Methods & Research*, *3*(1), 49–53. http://doi:10.1177/0049124117729700

Thomas, D. R. (2016). Feedback from research participants: Are member checks useful

in qualitative research? *Qualitative Research in Psychology, 14*(1), 23-41. https://doi:10.1080/14780887.2016.1219435

Thompson, N., Mcgill, T. J., & Wang, X. (2017). Security begins at home: Determinants of home computer and mobile device security behavior. *Computers & Security, 70*, 376-391. https://doi:10.1016/j.cose.2017.07.003

Thomson, R., & Mcleod, J. (2015). New frontiers in qualitative longitudinal research: An agenda for research. *International Journal of Social Research Methodology, 18* (3), 243-250. https://doi:10.1080/13645579.2015.1017900

Thornton, I. (2018). Malicious attacks and actors: An examination of the modern cyber-criminal. *Edpacs, 57*(1), 17-23. https://doi:10.1080/07366981.2018.1432180

Tomkinson, S. (2014). The impact of procedural capital and quality counsel in the Canadian refugee determination process. *International Journal of Migration and Border Studies, 1*(3), 276. http://doi:10.1504/ijmbs.2014.068969

Tong, F., & Yan, Z. (2017). A hybrid approach of mobile malware detection in Android. *Journal of Parallel and Distributed Computing, 103*, 22-31. http://doi:10.1016/j.jpdc.2016.10.012

Tran, T. V., & Ahn, H. (2017). Challenges of and solution to the control load of stateful firewalls in software-defined networks. *Computer Standards & Interfaces, 54*, 293-304. https://doi:10.1016/j.csi.2017.01.012

Tsai, A. C., Kohrt, B. A., Matthews, L. T., Betancourt, T. S., Lee, J. K., Papachristos, A. V., & Dworkin, S. L. (2016). Promises and pitfalls of data sharing in qualitative research. *Social Science & Medicine, 169*, 191-198.

https://doi:10.1016/j.socscimed.2016.08.004

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programs in organizations. *European Journal of Information Systems, 24*(1), 38-58. https://doi:10.1057/ejis.2013.27

Twining, P., Heller, R. S., Nussbaum, M., & Tsai, C. (2017). Some guidance on conducting and reporting qualitative studies. *Computers & Education, 106,* 115-128. https://doi:10.1016/j.compedu.2016.12.002

Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. *Computers & Security, 81,* 123–147. https://doi:10.1016/j.cose.2018.11.001

U.S. Department of Health & Human Services. (1979). *The Belmont Report*. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Vallano, J. P., Evans, J. R., Compo, N. S., & Kieckhaefer, J. M. (2015). Rapport-building during witness and suspect interviews: A survey of law enforcement. *Applied Cognitive Psychology, 29*(3), 369-380. https://doi:10.1002/acp.3115

Venkatesh, V., Brown, S., & Sullivan, Y. (2016). Guidelines for conducting mixed-methods research: An Extension and illustration. *Journal of the Association for Information Systems, 17*(7), 435–494. https://doi:10.17705/1jais.00433

Venkatraman, S. (2017). Autonomic framework for IT security governance. *International Journal of Managing Information Technology, 9*(3), 1-11. https://doi:10.5121/ijmit.2017.9301

Vitak, J., Proferes, N., Shilton, K., & Ashktorab, Z. (2017). Ethics regulation in social computing research: Examining the role of institutional review boards. *Journal of Empirical Research on Human Research Ethics, 12*(5), 372-382. https://doi:10.1177/1556264617725200

Vitak, J., Shilton, K., & Ashktorab, Z. (2016). Beyond the belmont principles: Ethical challenges, practices, and beliefs in the online data research Community. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing - CSCW 16, 2*(2), 941–953. https://doi:10.1145/2818048.2820078

Wang, Z., Wang, N., Su, X., & Ge, S. (2016). Differentiated management strategies on cloud computing data security are driven by data value. *Information Security Journal: A Global Perspective, 25*(4-6), 280-294. https://doi:10.1080/19393555.2016.1231353

Watson, R. (2015). Quantitative research. *Nursing Standard, 29*(31), 44-48. https://doi:10.7748/ns.29.31.44.e8681

Weger, U., & Wagemann, J. (2015). The challenges and opportunities of first-person inquiry in experimental psychology. *New Ideas in Psychology, 36,* 38-49. https://doi:10.1016/j.newideapsych.2014.09.001

Weller, S. (2017). Using internet video calls in qualitative (longitudinal) interviews: Some implications for rapport. *International Journal of Social Research Methodology, 20*(6), 613-625. https://doi:10.1080/13645579.2016.1269505

White, D., & Hind, D. (2015). Projection of participant recruitment to primary care

research: A qualitative study. *Trials, 16*(1), 103-117. https://doi:10.1186/s13063-015-1002-9

Wilson, A. D., Onwuegbuzie, A. J., & Manning, L. P. (2016). Using paired depth interviews to collect qualitative data. *The Qualitative Report*, *21*(9), 1549-1573. Retrieved from https://nsuworks.nova.edu/tqr/vol21/iss9/1

Wilson, J., Mandich, A., & Magalhães, L. (2015). Concept mapping. *Qualitative Health Research, 26*(8), 1151-1161. https://doi:10.1177/1049732315616623

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816. https://doi:10.1016/j.chb.2008.04.005

Yan, F., Jian-Wen, Y., & Lin, C. (2015). Computer network security and technology research. *2015 Seventh International Conference on Measuring Technology and Mechatronics Automation*, *5*(2), 151–178. https://doi:10.1109/icmtma.2015.77

Yang, H., Wang, X., Yang, C., Cong, X., & Zhang, Y. (2019). Securing content-centric networks with content-based encryption. *Journal of Network and Computer Applications, 128,* 21-32. https://doi:10.1016/j.jnca.2018.12.005

Yang, S. (2018). Analysis of the reliability of a computer network by using an intelligent cloud computing method. *International Journal of Computers and Applications, 41*(4), 306-311. https://doi:10.1080/1206212x.2017.1417770

Yao, M., Chuang, M., & Hsu, C. (2018). The Kano model analysis of features for mobile security applications. *Computers & Security, 78,* 336-346.

https://doi:10.1016/j.cose.2018.07.008

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation, 19*(3), 321-332. https://doi:10.1177/1356389013497081

Yin, R. K. (2014). *Case study research: Design and methods*. Sage.

Yin, R. K., & Campbell, D. T. (2018). *Case study research and applications: Design and methods*. Sage.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security, 55*, 81-99. https://doi:10.1016/j.cose.2015.06.011

Zhang, Y., Chen, X., Li, J., Wong, D. S., Li, H., & You, I. (2017). Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. *Information Sciences, 379*, 42-61. https://doi:10.1016/j.ins.2016.04.015

Zhou, L., Fu, A., Yu, S., Su, M., & Kuang, B. (2018). Data integrity verification of the outsourced big data in the cloud environment: A survey. *Journal of Network and Computer Applications, 122*, 1-15. https://doi:10.1016/j.jnca.2018.08.003

Zhou, Y., & Yang, B. (2017). Continuous leakage-resilient certificate less public key encryption with CCA security. *Knowledge-Based Systems, 136*, 27-36. https://doi:10.1016/j.knosys.2017.08.019

Zota, R. D., & Ciovica, L. (2015). Designing software solutions using business processes. *Procedia Economics and Finance, 20*, 695-699. https://doi:10.1016/s2212-5671(15)00125-2

Appendix: Interview Questions

Interview: Mobile network infrastructure security in developing countries – A Kenya case study

Name:_____

Date: _____

Time:_____

1. What strategies have you used to protect the mobile network infrastructure from cyberattacks in your organization? Of the strategies that you just mentioned, would you like to elaborate on what made them useful?
2. What other strategies did you deploy to protect the mobile network infrastructure that was not successful, and would you mind elaborating why they were not successful?
3. Of the strategies that you used to protect the mobile network infrastructure, which ones were effective? In your opinion, what made those strategies effective?
4. While planning on the strategies to use to protect the mobile network infrastructure, was the principal of defense-in-depth considered? If yes, would you like to elaborate further on what you will take into consideration? If not, would you elaborate on why?
5. What consideration are application security and data security afforded in the strategies you settled on to protect the mobile network infrastructure from cyberattacks?

6. What part does the use of policies, procedures, and security awareness play in the overall strategies for protecting the mobile network infrastructure from cyberattacks?
7. In your opinion, how do mobile network infrastructure management and governance factor into the overall strategies you deployed to protect the mobile network infrastructure?

Concerning the Interviews:

- I will paraphrase all the partakers' answers to confirm accuracy (e.g., What I understood is that; From what I got is that, etc.).