2022

Strategies to Secure a Voice Over Internet Protocol Telephone System

Sherese Bernard
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Sherese Bernard

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

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

Walden University
2022

Abstract

Strategies to Secure a Voice Over Internet Protocol Telephone System

by

Sherese Bernard

MS, Walden University, 2014

BS, Walden University, 2012

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

March 2022

Abstract

Voice over internet protocol (VoIP) provides cost-effective phone service over a broadband internet connection rather than analog telephone services. While VoIP is a fast-growing technology, there are issues with intercepting and misusing transmissions, which are security concerns within telecommunication organizations and for customers. Grounded in the routine activity theory, the purpose of this multiple case study was to explore strategies information technology (IT) security managers used to secure VoIP telephone systems in telecommunication organizations. The participants consisted of nine IT security managers from three telecommunication organizations in New York who possessed the knowledge and expertise to secure a VoIP telephone system. The data were collected using semi structured interviews, note taking, and one document from one organization. Four themes emerged from the thematic analysis: best practices for VoIP security, using a secure VoIP provider, VoIP security recommendations, and awareness of future security concerns. A key recommendation for IT security professionals is to ensure encryption to secure a VoIP telephone system. The implications for positive social change include the potential for IT security managers and telecommunication organizations to reduce data breaches and the theft of their customers' identities and credit card information.

Strategies to Secure a Voice Over Internet Protocol Telephone System

by

Sherese Bernard

MS, Walden University, 2014

BS, Walden University, 2012

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

March 2022

Dedication

I am dedicating this study to God. He has given me the strength and the knowledge to achieve all obstacles that have come my way during my doctoral journey. To my love, Charles, thank you for believing in me. To my daughters Shaniqua and Leeyah, who have been there with me and understood that mommy had work to accomplish, you girls have always been the light at the end of the tunnel, which motivated me to want more and be more for you two. As I continued earning my degrees, I had to show you what it is to be the first in the family to want something so bad that it hurts. You girls saw me studying and researching many nights, working hard to make my accomplishments and dreams a reality. I want you girls to know that anything you put your heart, mind, and soul into, you can achieve it. Mommy Loves You! I would also like to dedicate this study to my family and friends who became family during this journey. This study would not be possible without your encouragement and support.

Acknowledgments

I want to thank my chair member, Dr. Jodine Burchell, for being the mentor that I needed. She supported and helped me through some tough times. I will forever be grateful that you believed in me when I didn’t believe in myself. To my second committee member, Dr. Gary Griffith, and my URR, Dr. Bob Duhainy, thank you for supporting me.

To my sister, Tonia Hill, God rest her soul who always said to me, “Rese, you are going to learn until you cannot learn anything new.” Tonia was the one person that told me that I could do anything I wanted, and I should keep going until I could not go anymore because she wished she did. I know you are smiling down from heaven. To my grandparents, Brigadier Lebert and Valcena Bernard, I know you are proud of me and are rejoicing in heaven to my success. To my mother, Saundra Bernard, thank you for continuously checking in and believing in me. To my aunt, Barbara Bernard, thank you for those Saturday morning calls telling me I can do it when I thought I had nothing left to give. I want to thank all my family members. I want to thank all my friends that I made on this journey for always making sure that I was writing. To all the Walden classmates that had given me feedback when the words on the paper all looked the same, all of you have made me what I am today, which is better, and I Thank You.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Background of the Problem

Voice over Internet Protocol (VoIP) started as an experiment in 1973 to create inexpensive and reliable phone systems for organizations, but the developers did not focus on the security risks (Ukhaneva, 2015). The high demand and integration of VoIP into the mainstream have created a concern about the security of VoIP transmissions due to the possibility of the interception of voice data between one person to another over the internet (Patel, 2016). Satapathy and Livingston (2016) demonstrated that attackers eavesdrop on unsecured transmissions to gain personally identifiable information. Understanding the strategies New York telecommunication companies use to secure VoIP systems may help secure personal customer information. In this study, I focused on understanding the security aspects of VoIP and how IT security managers secure VoIP systems for telecommunication companies.

Problem Statement

Telecommunication organizations using VoIP telephone services have security vulnerabilities that can detrimentally affect their customers (Coates, 2016). Twenty-five percent of VoIP telecommunication organizations have reported unauthorized access to their customer’s personal information (Kim et al., 2015). The general IT problem was that some telecommunication organizations have problems securing their VoIP telephone systems, which causes an increase in data breaches. The specific IT problem was that some IT security managers in telecommunication organizations lack strategies to secure a VoIP telephone system from data being intercepted and misused.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies that IT security managers in telecommunication organizations use to secure a VoIP telephone system to stop data from being intercepted and misused. The population for this study was IT security managers employed by three telecommunication companies in New York that have strategies to secure a VoIP telephone system from data being intercepted and misused. The implications for a positive social change include that the strategies may reduce identity and credit card theft from data breaches.

Nature of the Study

For this study, I considered qualitative, quantitative, and mixed methods to help facilitate the research. Researchers use the qualitative method to gain an in-depth understanding of a phenomenon by capturing individuals' perspectives and experiences with the research subject (Birt et al., 2016). The qualitative method was appropriate for this study because it provided tools for an in-depth exploration of strategies to secure a VoIP telephone system. Quantitative researchers create a statistical analysis of numerical and experimental data under a reductionist, rational, and strictly unbiased paradigm (Leung, 2015). However, to answer the research question of this study, statistical analysis was not needed, so I did not employ the quantitative method. The mixed-method approach comprises quantitative and qualitative methods to fully explore the research topic (Abro et al., 2015). However, the lack of statistical analysis required to address the research question made the mixed-method approach unsuitable for this study. Instead, I used the flexibility of the qualitative method to analyze the contextually detailed responses of IT security managers.

I considered case study, narrative, and phenomenology for this qualitative study as possible research designs. A researcher uses the multiple case study design to perform an in-depth investigation of a group of people in an organization with a mixture of ideas (Salamzadeh et al., 2017). A multiple case study involves collecting and comparing data between multiple entities, which helps create themes relevant to similar types of organizations (Bogers et al., 2017). A multiple case study design was appropriate for this study because I used the data gathered from specific organizations to provide meaningful information regarding securing a VoIP system. The narrative design helps describe significant events or experiences within the participants' lives, including understanding what those experiences mean for them (Willgens et al., 2016). This study did not focus on individual experiences, so I did not employ this design. A phenomenological design involves observing individuals that experienced a phenomenon to gain their lived experiences (Matua, 2015). The research question does not revolve around the lived experiences of individuals or a group, so I declined to use this design. A multiple case study design was appropriate to investigate the problem, allowing for in-depth research of the strategies for securing a VoIP telephone system in telecommunication organizations.

Research Question

What strategies do IT security managers use in telecommunication organizations to secure a VoIP telephone system from data being intercepted and misused?

Interview Questions

1. What is your IT background in VoIP?
2. What methods have you used to secure a VoIP system?
3. What method or methods did you use that worked best to secure a VoIP system, or is there a specific way that the organization wants you to secure a VoIP system?
4. How did the security methods secure the VoIP system?
5. Which security methods work best?
6. What are the multiple ways of securing a VoIP system? If any?
7. How many managers or IT personnel are authorized to maintain the VoIP system?
8. How do you maintain a VoIP system?
9. How do you identify if the system is being compromised?
10. What steps are you taking to recognize the severity of the attacks?
11. Are there different levels of attacks?
12. What are the roles of all the people that take part in getting the system under control?

Conceptual Framework

The conceptual framework used in this study was the routine activity theory (RAT). Cohen and Felson (1979) proposed the RAT to study the patterns of crime committed and the people or items involved, determining the situation of a crime across time and space. Cohen and Felson asserted that a motivated offender, who commits a crime against a target, and a guardian, who protects against the offenders, must be present for the crime to occur. The RAT focuses on the structure that motivates criminals and decreases the risk of a crime by preventing it before it happens (Song et al., 2015).

The RAT applies to how a criminal carries out a routine activity and how the crime can be prevented (Zaslawski, 2017). Jitters, packet loss, and latency can allow hackers to intercept VoIP telephone services and access customer information (El Kafhali & Hanini, 2017). This interception may result in a criminal obtaining private information, including credit card information (Westlake, 2017). Using the RAT as the conceptual framework in this study helped me analyze the strategies IT security managers (i.e., guardians) put into place to thwart attackers (i.e., criminals) from obtaining data illicitly. The framework of the RAT provided a foundation for understanding the strategies for securing VoIP by allowing me to analyze how IT security managers detect patterns of criminal activity and prevent it. Additionally, the RAT aided in exploring how customers' data are compromised and how IT security managers may reduce that risk.

Operational Definitions

I am providing the following definitions of terms used in the study so the reader can clearly understand them. The four operational definitions are related to VoIP.

Eavesdropping: The act of secretly listening to a conversation without the party's consent in the communication (Cha et al., 2017).

Man-in-the-middle (MITM) attack: Malicious users intercept communication between nodes (Alaba et al., 2017).

Telecommunication organization: An organization that provides services, such as telephone and internet, permitting global communication (Noh et al., 2016).

VoIP: A protocol facilitating communication by transmitting voice and video communication over the internet protocol (Irshad et al., 2015).

Assumptions, Limitations, and Delimitations

This subsection includes a discussion of this study's assumptions, limitations, and delimitations. These areas factored into the foundation of the study, including in the data collection and analysis processes. I used the assumptions and limitations to define areas that created an issue while setting boundaries to restrain it with delimitations.

Assumptions

Assumptions are facts considered correct without verifying (Erwin et al., 2015). First, I assumed IT security managers would answer all interview questions thoroughly and truthfully. Another assumption was that the IT security managers would provide meaningful information related to the strategies used for securing a VoIP telephone system without personal bias to the interview questions. Lastly, I assumed the study's conceptual framework reflected the VoIP telephone crimes and was clearly defined.

Limitations

Limitations are deficiencies or restrictions that limit the realism in the research (Busse et al., 2017). First, one potential limitation was that company policy might have restricted what IT security managers divulged due to possible security risks. Second, the responses from the IT security managers about the strategies being used to secure a VoIP system may not have been clearly understood by me. Lastly, by limiting the source of participants to only three telecommunication organizations, I may not have been able to fully explore the strategies used across the telecommunications field to secure a VoIP system.

Delimitations

Delimitations define the scope of the research study that is within the researcher's control (Rosenberg & Koehler, 2015). First, the three participating telecommunication organizations were located in New York state. I selected three IT security managers that use a VoIP system as participants, but they may not have known to recognize the severity of a data attack. Lastly, the focus of the study was limited to the strategies used to protect against VoIP telephone fraud.

Significance of the Study

Contribution to IT Practice

There was minimal research regarding strategies to secure a VoIP telephone system, which created an opportunity to enhance the knowledge and practice in this area. This study contributes to IT practice by exploring the strategies of telecommunications companies in New York state to secure voice communications to prevent unauthorized data interceptions. Organizations use VoIP as a data and voice communication technology through public and private networks, creating opportunities for MITM attacks to collect private information from unsuspecting callers (Bensalah et al., 2017; Conti et al., 2016; Park, 2007). IT security managers may use the strategies found in the current study to enhance their practice of securing VoIP communication, avoiding exposing private data to unknown entities.

Implications for Social Change

The implications for positive social change include that the strategies collected in this study may reduce identity and credit card theft for customers. While social engineering is a common tactic for obtaining identifiable information, attackers also use MITM attacks to eavesdrop on confidential conversations containing private information (Haggag, 2017). Since customers are unaware of a third party listening, they disclose personally identifiable information intended for the customer service agent that an attacker intercepts. The attackers listen to the calls, gathering information, such as the mother's maiden name, social security numbers, and credit card information, to commit a crime against the customer (Clough, 2015). Securing a VoIP system in telecommunication organizations may reduce identity theft for customers and keep their information secure.

A Review of the Professional and Academic Literature

This literature review includes in-depth information related to the central research topic, including critical analysis and synthesis of journal articles concerning VoIP telephone systems and the RAT conceptual framework. I begin with a discussion of the RAT framework and other frameworks that were considered, such as the lifestyle exposure theory (LET) and lifestyle routine activity theory (LRAT). Then, the existing literature on previous strategies for securing VoIP systems, VoIP security breaches, and successful strategies to prevent VoIP breaches are reviewed. I organized the literature review around the following themes to explain the severity of securing a VoIP system in telecommunication organizations: (a) conceptual framework, (b) history of VoIP, (c)

VoIP usage, (d) VoIP impact, (e) VoIP security concerns, (f) data breaches, (g) VoIP security strategies, (h) future direction of VoIP, and (i) telecommunication organizations. Information from the peer-reviewed articles included in this chapter will help the reader better understand the strategies that IT security managers use to prevent a VoIP attack against telecommunication organizations in New York.

The literature review includes 200 articles, government websites, and journals as sources, of which 189 (92%) were peer reviewed, and 185 (85%) were published within 5 years of my expected graduation date. The references in this study have been verified through *The Ulrich's Global Serials Directory*, a source that verifies that academic journals, e-journals, magazines, and newspapers are peer reviewed. I located the articles through ACM Digital Library, ProQuest Central, Google Scholar, Science Direct, IEEE Xplore Digital Library, Walden University Library, and Thoreau Multi-Database search. The keyword search terms used were: *VoIP, VoIP security, VoIP telecommunications, RAT, LET*, *LRAT, VoIP benefits, VoIP threats, Telecommunication organizations, VoIP breaches, securing a VoIP system,* and *cybersecurity.*

Conceptual Framework

Cohen and Felson (1979) proposed the RAT to assist in illustrating the patterns of crimes committed and explains criminal events through asserting three factors necessary to examine a crime: (a) a motivated offender, (b) a victim, and (c) the absence of a guardian tasked with preventing crimes. Song et al. (2015) indicated that the RAT approach focuses on the structure that motivates criminals and is used to decrease the risk of a crime by preventing the crime before it happens. The RAT applies to crimes involving a VoIP telephone system in telecommunications organizations, including the misuse of call information being intercepted and recorded. In the context of VoIP systems, IT security managers are the guardians who seek to prevent criminal activity on their network. The customers are the intended victims of the attacker. Additionally, the crime focused on this study is telephone fraud, which Westlake (2017) suggested occurs when attackers use MITM attacks on VoIP transmissions. All the components in the RAT can be applied to the criminal activity that takes place in a VoIP system.

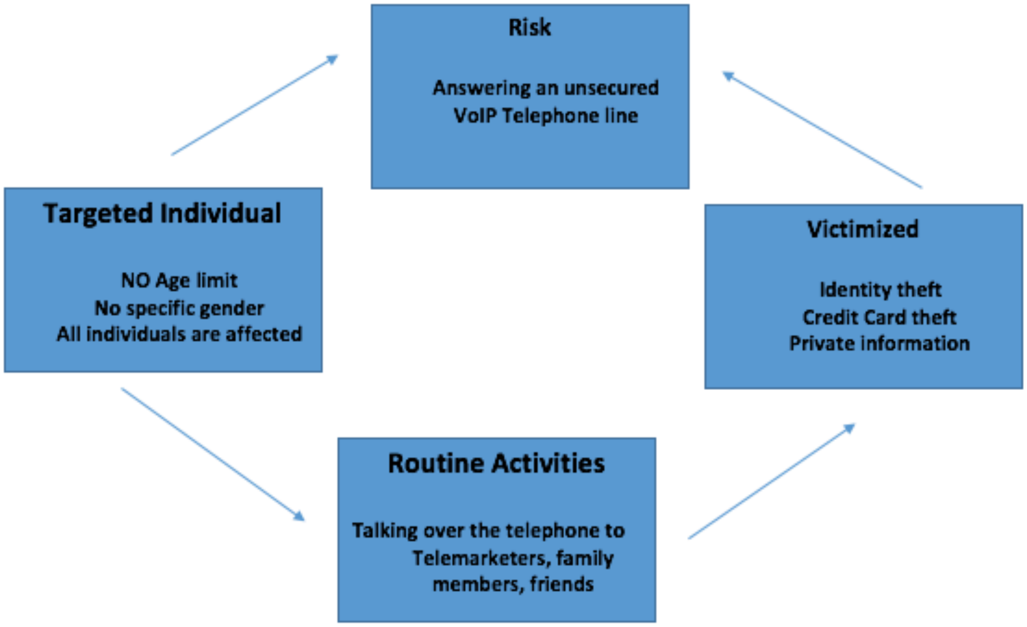
The goal of detecting patterns is to mitigate problem areas in the future. Argun and Dağlar (2016) and Leukfeldt and Yar (2016) reached a similar conclusion that the RAT may help determine how to prevent crime from happening. Therefore, I used the RAT framework as a foundation for understanding the strategies for securing VoIP by analyzing how IT security managers prevent and detect criminal activity patterns and assume guardians' roles in protecting systems from illicit use. Cohen and Felson (1979) explained that the guardian is an implicit role that is often the neglected element in crime but found that the absence of a capable protector increases the rate of criminal activity. Milzcik (2015) reaffirmed that the absence of a guardian motivates criminals more than areas with a capable guardian. A capable IT security manager must reduce illicit activities committed on VoIP systems, including analyzing and implementing strategies to prevent hackers from accessing the transmissions.

In the case of this study, the motivated offenders of the RAT are the hackers committing crimes such as telephone fraud. Cohen and Felson (1979) described that motivated offenders will commit crimes against a victim, including stealing private information for personal gain. Leukfeldt and Yar (2016) extended this concept to IT by stating the criminal will find a suitable target and strike when the opportunity presents itself, including when the victim logs into their computer. In this context, the victim will use an unsecured VoIP line at a telecommunications service, and the criminal will capture the private information when this occurs.

Customers who use VoIP service and had a criminal intrude on their conversation are victims in this context. Zaslawski (2017) concluded that offenders reach their targets and collect information using the internet without the consumers being aware. Choi et al. (2016) indicated that the internet attracts computer criminals to victims because of a lack of enforceable consequences due to a lack of boundaries. Cohen and Felson (1979) defined the ability to escape the consequences of criminal activity as accessibility. A routine activity, such as contacting a telecommunication company to pay bills over the phone, can cause a targeted person’s personal information to be stolen (see Figure 1).

Figure 1

A Targeted Individual Doing a Routine Activity While Being Victimized


Risk
Answering an unsecured VoIP Telephone line
Targeted Individual
NO Age limit
No specific gender
All individuals are affected
Victimized
Identity theft
Credit Card theft
Private information
Routine Activities
Talking over the telephone to Telemarketers, family members, friends

The routine activity has influenced telecommunication organizations that use VoIP systems because of computer crimes in organizations. Reyns et al. (2015) noted there are many victims of computer crimes, in which attackers invade systems to gain access to these targets. Gavilanez et al. (2017) reported that attackers take control when they gain unauthorized access to VoIP systems, which allows them to manipulate and configure the signaling to commit their crime. The RAT was useful to help evaluate the patterns and strategies of illicit attacks on VoIP infrastructures.

Evolution of the RAT

Many different conceptual frameworks have shown how technology has evolved into what it is today, such as improvements, cost, and security. Cohen and Felson (1979) created RAT to show how crime is not affected by unemployment, change, or economic recession; crime happens because of an individual’s behavior. The RAT shows that it is the routine activity of a person’s everyday lifestyle that puts them at a higher percentage of committing a criminal act. In the RAT, Cohen and Felson explained why certain types of crimes happen more often than other crimes. The RAT has evolved to provide solutions to criminal problems as well as address modern crimes like cyberattacks. While Leukfeldt and Yar (2016) noted the traditional use of the RAT for studying traditional crimes, such as burglary, homicide, and theft, Vakhitova et al. (2015) and Llinares (2015) explained that the RAT has also been used to study cybercrimes and its influences. Song et al. (2015) theorized that cybercriminals target individuals who use the internet to pay bills and shop, while Llinares emphasized that risk factors include using information and communication technologies. The increase in cybercrime indicates the need to study strategies to secure VoIP telephone systems.

Researchers have used the RAT to study cybercrimes because of the use of new communication technology. Leukfeldt and Yar (2016) applied the RAT to understand cybercrime in three ways: computer-focused, financial, and interpersonal crimes. Reyns and Henson (2016) focused on the likelihood of a victim experiencing identity theft online, contributing to billions of dollars in financial losses for victims. Choi and Lee (2017) concluded that cybercrime occurs when attackers gain access to digital information, which differentiates it from other researched areas in traditional crimes. Use of the RAT has evolved to cybercrimes because of the growth of technology.

Critical Analysis

The key tenet of the RAT is that crime occurs when a motivated offender attacks a suitable target without a capable guardian (Merien et al., 2018). Peterson and Densley (2017) found that the RAT can be used to explain how crimes take place online with many people connecting online every day, which is customary for today's society. Pratt and Turanovic (2016) viewed the RAT as a lifestyle theory that describes a person's events to protect them from being at risk of becoming a victim. Researchers can use the RAT to help others avoid becoming victims by eliminating elements (i.e., a suitable target, a motivated offender, and the guardian). Reyns and Henson (2016) found that people become victims because of the time spent online and the activities that people are doing online (i.e., checking bank information, shopping, and paying bills) can put a person at risk for being victimized.

However, there are contrasting views of the effectiveness of the RAT. Pratt and Turanovic (2016) noted that the RAT does not focus on behaviors that place a victim at risk. Ashby and Tompson (2017) found that the necessity of the three items (i.e., motivated offender, a targeted person, and the absence of a guardian) limits identifying potential crimes that are missing one of those components. Furthermore, Schaefer and Mazerolle (2017) argued that the RAT has not addressed how the three controllers distinguish between the different types of crimes that may take place. These are critical elements to consider when considering employing the RAT.

RAT Influences on VoIP Security Strategies

The RAT provides a foundation for a person or organization to participate in the crimes associated with VoIP attacks. Abouelmehdi et al. (2018) insisted that an attacker might hijack a VoIP call by eavesdropping to gain personal information. In this study, I used the RAT to address the VoIP computer crimes in telecommunication organizations because the framework explains why the motivated offender (i.e., hackers) would want to victimize the suitable targets (i.e., customers) and how the guardian (i.e., IT security managers) can help to secure a VoIP system in telecommunication organizations from being compromised.

Hawdon et al. (2017) found that the use of the RAT was extended because of cyber victimization and the influences that crime has on the online community. Ghazali et al. (2016) insisted that securing a VoIP system has been a significant concern and should be addressed. The routine activity of paying bills or using a credit card over the phone could reduce the idea of crimes occurring if a customer understood the consequences. Using the RAT in this study gives the reader an idea of how crimes are committed to the customers in telecommunication organizations that use a VoIP system.

Analysis of Contrasting Theories

In researching the RAT, I found some contrasting theories that researchers identified. There are many theories related to IT and securing the use of a VoIP system (Skopik et al., 2016). Theories considered in this literature review are LET and the situational crime prevention (SCP) theory because they address the security of VoIP systems and how computers in a telecommunication company can be used to victimize a customer. These contrasting theories can address the issues with maintaining and securing a VoIP system, but I did not choose them for this study.

LET. Hindelang et al. (1978) developed the LET framework in 1979 to explain that a person’s lifestyle may lead to personal victimization. A person’s lifestyle may be patterned, allowing the individual to use their time and energy in routine activities that may conclude in a crime (Hindelang et al., 1978). Hindelang et al. developed the LET survey victim patterns of people (ages 12 and older) to discover why they become victims of the proposed crimes and find discrepancies in the risk of violence for victims in different age groups. The LET was also used to distinguish if a victim’s day-to-day routine can put them at risk of a criminal act. The LET helps researchers focus on how a person's lifestyle can expose them to becoming victims of a crime; however, the victim’s lifestyle may factor into their VoIP victimization if it is outside of their control, so this theory was not adequate address the needs of the study.

SCP Theory. Clarke (1980) developed the SCP to explore why offenders commit acts of crimes and understand the thought process of how criminals commit crimes to create methods to prevent future crimes from happening. The SCP theory is intended to change how criminals think about committing a crime and making a person a victim (Tunley et al., 2017). For example, providing software that will allow people to press their credit card information on their telephone keypads instead of verbally announcing the numbers aloud to a telemarketer in a telecommunication organization. This example should reduce the crime of a hacker gaining personal information from a customer paying a bill over the phone. Clarke (2018a) created the theory to focus on the opportunity to reduce and avoid new crimes from happening by putting a stop to a crime by preventing it from happening in the first place. The SCP theory is primarily used by researchers who want to understand why, where, and how a crime occurs to avoid it. The focus of the current study was on the strategies IT security managers use to secure a VoIP system to reduce criminal activity; therefore, I did not use the SCP theory to observe why a hacker would commit a crime and try to change the hacker's perceptions to prevent the crime.

Analysis of Supporting Theories

RAT's supporting theories inform when researchers want to know why offenders commit crimes and become criminals and how victims can prevent them from becoming victimized. The two theories chosen for this section were the LRAT and the technology-enabled crime, policing, and security theory. The supporting theories can address the risks that criminals take and how people can become victims of a VoIP system but were not chosen as a theory for this study.

Lifestyle Routine Activity Theory. Cohen et al. (1981) created LRAT to identify victim properties by exposure, proximity, attractiveness, guardianship, and definitional properties of crimes. Exposure to a potential offender is likely that there will be a greater risk of becoming a victim (McNeeley, 2015). Proximity signifies being near a motivated offender, putting a victim at risk (McNeeley, 2015). Attractiveness refers to a person's desirability and what attracts the victimizer to their victim (McNeeley, 2015). An example of attractiveness can also be financial seeing a person's bank information can make people a target against credit card theft. Guardianship prevents crime by being present or acting to protect a person or an idea from being victimized (McNeeley, 2015). LRAT explains crime as an event because of everyday activities such as work, school, or going for a walk. The daily behavior may affect the likelihood of a crime taking place.

Hindelang et al. (1978) insisted the extent of a person's lifestyle can expose them to places and people where crimes occur.

RAT and LET have been combined into LRAT to signify a person’s lifestyle and routine activities that have opened opportunities to becoming a victim. LRAT is considered as a supported theory to RAT. Miethe and Meier (1990) proposed LRAT to determine that a person’s lifestyle will make them a victim. LRAT is a routine activity that may elevate a person’s odds of becoming a victim. LRAT and RAT are similar theories that need to have three components a motivated offender, an attractive target or victim, and the absence of a capable guardian to create a victimized event (Pratt & Turanovic, 2016). The LRAT and RAT theories differ because LRAT focuses on a person’s behaviors and describes a person’s activities. Vakhitova et al. (2015) explained that LRAT and RAT are designed to explain the varieties of risk in victims. LRAT exposes people that participate in bad behaviors. Weulen Kranenbarg et al. (2017) emphasized that the odds of engaging in behaviors such as robbing, taking drugs, and computer hacking or stealing elevates the chances of becoming a victim. An example of LRAT is a person walking alone at night, which puts them at a higher risk of being victimized than a group of people walking together

Technology-Enabled Crime, Policing, and Security Theory. McQuade developed the technology-enabled crime, policing, and security theory in 1998 to focus on why crimes occur with the innovative use of technology. McQuade (1998) assumed that if he knows the technical nature of the criminal's potential threats, he can control desired behavior to commit a technology crime. The technology-enabled crime theory monitors the use of crime waves that recognize or understands the intensity of a crime (McQuade, 2001). The crime waves can measure, compare, and predict a threat posed by cybercrime and take security measures to prevent or control the crime from happening. The theory applies to internet crimes because people take advantage of new technology that allows them to be anonymous to the user (Adah Agana & Wario, 2018). Technology-enabled crime, policing, and security theory supports VoIP crimes committed over the internet and is very hard to detect who is committing the crime until the crime has already happened.

Analysis of Potential Themes and Phenomena

The attacks on VoIP telephone systems require understanding how it functions and the services used. For instance, security strategies are needed to target specific functions of the VoIP system. Hence, exploring VoIP usage, privacy, and security challenges is necessary to bring the theory into context.

VoIP. VoIP was created to transmit and receive digital voice traffic using a data network, which would replace public switch telephone networks (Miraz et al., 2017). Transmitting telephone calls over an IP network instead of using a public switch telephone network made sending and receiving phone calls easier. Shaw and Sharma (2016) indicated VoIP signaling controls telephony communication by using the internet. Therefore, VoIP users, such as professionals, academic institutions, and home users, adopted the new technology as it eliminated the use of many devices (Montazerolghaem et al., 2017). Organizations use VoIP because it cuts costs and uses a landline phone line, making it easier to use an internet connection on a computer to work and receive phone calls.

VoIP is used to transfer communication messages between networks. VoIP receives attention from businesses and general users because of cost-efficiency and adaptability; however, it also has significant security dangers (Safoine et al., 2018). Jingi and Muhammad (2017) indicated that new VoIP being deployed on networks contains many security issues, which Chang et al. (2015) highlighted as the denial of service (DoS), the elevation of privilege, information disclosure, and repudiation, spoofing, and tampering. Souag et al. (2015) described VoIP as a containing system and application weakness for security exploits. VoIP has many security issues that justify the types of threats and the possible target of the threat for a VoIP system.

Jingi and Muhammad (2017) focused on the impacts of safety efforts on VoIP systems, which permits the deployment of a secured VoIP system to fail. The safety impacts that were not considered were the signaling and media transport protocols. Rajput and Barkatullah University Institute of Technology Bhopal, India (2017) indicated that the signaling and media protocols are used to set up and terminate calls. When VoIP deploys, there is a DoS risk. DoS danger will deny clients access to VoIP administrations, upset correspondence, and close power and movement to the business (Bhuyan et al., 2016). The vulnerabilities that complete distinctive measures of VoIP security assaults affect accessibility, secrecy, and trustworthiness. Abouelmehdi et al. (2018) indicated that a VoIP framework should have a secured VoIP convention and the utilization of VoIP-mindful to modify the IP network permitting a secured IP information system to send secure messages from individual to individual.

Azad et al. (2018) noted the utilization of VoIP and addressed the security worries for the future of VoIP. Yet, the attention is on what makes VoIP powerless and the need to locate a fast way to control the security dangers. Gupta and Jha (2015) explained that utilizing security dangers like encoding voice information through a VoIP system should secure a VoIP network and the firewalls that can secure and control attacks. Basem et al. (2015) concurred with Jingi and Muhammad (2017) that a VoIP network should have a standard method for securing a VoIP system. Basem et al. agreed that utilizing a multilayer secured Session Initiation Protocol (SIP) for an organization that uses VoIP is a safeguard against listening stealthily and assaults. The security of VoIP is essential as an organization uses the system to correspond over the World Wide Web.

VoIP allows telecommunication companies to make phone calls over a broadband internet connection instead of a typical analog telephone line. Shoket and Aulakh (2018) indicated VoIP works with digitalizing voice data packets which send and receive voice messages through the internet, allowing fewer fees for essential broadband services and faster internet connections. As the technology of VoIP seems to increase, and new users are arising every day, there will be new ways to compromise the VoIP technology (Bhuyan et al., 2016). Securing a VoIP system is vital for any organization to ensure that personal information is not compromised. According to Sasikala (2017), organizations should do security checks on their VoIP system to eliminate security assaults. The monitoring of VoIP systems should alert IT security managers, if an attack occurs on the system.

VoIP usage in Telecommunication Companies

The benefits of VoIP services provide telecommuting operators with the ability to use call waiting, conference calling, call transfer, caller ID, and a wide array of VoIP services from using an internet protocol. Azad et al. (2018) indicated the cost of using VoIP plays a great deal in the benefits of adopting VoIP services as it is cheaper to have a VoIP system. A VoIP telephone system can save the company money from paying for a circuit-based switch, which requires a dedicated line. Raheja and Munjal (2015) explained that the key benefits of VoIP services are reliable and cost-efficient. Azad et al. (2018) and Raheja and Munjal emphasized that using a VoIP system is the easiest way to make phone calls. Jalendry and Verma (2015) noted that more organizations are adopting the technology with innovation in VoIP technology. The evidence shows that more organizations are turning to the new technology because of lower costs and excellent call quality.

VoIP allows telecommunication companies to make phone calls over a broadband internet connection instead of a typical analog telephone line. Dohler et al. (2017) indicated a VoIP system works with digitalizing voice data packets that send and receive voice messages through the internet. Devi et al. (2015) described that organizations have better media access with VoIP because voice traffic goes over the internet, making it easier for colleagues to send instant messages, make voice-video calls, and trade pictures making VoIP media possible. Kolhar et al. (2017) indicated VoIP is reliable and cost-effective, and many organizations are switching from the old communication calls to VoIP calling. An organization that uses Skype and Google to communicate amongst employees saves money by lowering the cost of their telephone bills.

VoIP Deployment Model

VoIP has a relationship with the seven-layer Open Systems Interconnection (OSI) Model. The OSI model was developed by the International Organization of Standardization in 1984 to ensure data communication worldwide (Bravo & Mauricio, 2018). The OSI model communicates to all the layers above and below to show an understanding of technology and how it works together in the model. The model divides layers to help pinpoint areas of error and help to minimize future boundaries between the layers (Oliveira et al., 2019). The seven layers are the application, presentation, session, transport, network, data link, and physical.

Application*,* which is the seventh layer and closest to the end-user, interacts directly with software applications. The application layer communicates with data to allow communication to exist (Fischer et al., 2017). The function of the application layer is to identify communication, accessibility, and synchronizing communication to transmit data (Chahid et al., 2017). Presentation, is the sixth layer, and its function is to make sure the transmitted data is readable by the application layer (Thiyagarajan & Raveendra, 2017). The presentation layer, called the syntax handles exchanging information between the two communicating systems (Sinha et al., 2017). Computers can translate data between networks and other machines. Session, fifth layer, is where VoIP signaling protocols operate. The session layer allows two users on different systems to begin communication (Zhao et al., 2018).

Layers four and five are where VoIP security can break. *Transport* is the fourth layer providing service to the session layer (Deart & Fatkhulin, 2017). The transport layer is an end-to-end layer and carries the conversation from the source to the destination. *Session*, the fifth layer is where connectivity between computers is controlled, and security should be at high alert. This layer is responsible for the close of sessions which is a check point for recovery. This layer ensures the operation of restarts and termination procedures (Nastase, 2017). *Network*, the third layer, delivers packets from user to destination across multiple networks (Kizza, 2017). The network layer breaks down the large packets into smaller packets to avoid congestion on the network. When packets travel from network to network, getting to their destination problems can emerge, such as different networks, large packets, and different protocols (Karakus & Durresi, 2017). *Datalink,* the second layer, transfers data between network to detect and correct any errors that may occur on the physical layer (Rani et al., 2017). The function of the data link layer is to focus on the local delivery of addressing media arbitration. *Physical,* the first and lowest layer on the OSI model ensures that bits are sent equally from one end of communication to the other (Oppitz & Tomsu, 2017). The concerns of this layer are transmission, timing, and signals, so the transmitter and the receiver are on the same levels.

VoIP is related to the OSI model because the model identifies the protocols used to transmit VoIP calls. Soni et al. (2017) agreed that each layer of the OSI model performs a job that relies on the layers below it for support while supporting the layer above it. The OSI model can be used to identify the protocols used to transmit VoIP. The OSI model shows how data moves from an application through a network to software onto another computer (Jacobson et al., 2017). The seven manageable layers are divided into tasks that will move telephone information in telecommunication organizations between networks. The layers are self-contained, so the layers are used independently so that when one layer is corrupt, it will not affect the other layers (Yarygina & Bagge, 2018). The OSI model gives an IT security manager an understanding of how a VoIP network works while grasping all sources that may help with troubleshooting, configuring, and designing the network.

VoIP Impact

Positive Impact. Online communication has changed from chat rooms, emails, and social networking using VoIP. Goodman-Deane et al. (2016) agreed that the use of internet percentage has grown because of making phone calls over the internet. Telecommunication organizations converted their analog voice calls into packets of data. Shaffer (2017) indicated with the changing technology of VoIP telecommunication industries were encouraged to initiate communication networks for their organizations. Telecommunication organizations use Session Initiation Protocol to deliver VoIP services that are cheaper. Bogoslavskyi and Stachniss (2017) explained that SIP delivers good voice quality for communication, making the voice calls perceptible and high quality. VoIP services for telecommunication organizations save money, and voice calls are clear.

Flexibility. The flexibility of VoIP allows voice packets to travel over a digital network. Zhang et al. (2016) indicated that VoIP flexibility could implement new applications that organizations can adopt VoIP services such as Skype and Gtalk. Organizations are using these VoIP services because they save the organization money. Miraz et al. (2015) explained the transmission of voice packets through a non shared reserved switched circuit allows the packets to have the freedom to arrive in any order. The packets arriving in any order give the flexibility of multiple routing of VoIP traffic. Shaw and Sharma (2016) described the flexibility of VoIP entices organizations to switch because VoIP provides an interactive communication service such as video and voice conferencing. VoIP data that is difficult to transfer helps to transfer a circuit-switched network to transmit voice signals over the internet.

Reduced cost. VoIP is a cheap and effective way of providing telephone services to an organization. Rojas et al. (2018) indicated that 31% of organizations use VoIP technology because of the total cost and savings to the company. Most organizations use free options associated with Google Voice and Skype. Tchernykh et al. (2019) described it is inexpensive to pass voice data through the organization's IP network, as broadband is cheap and easy to get. Also, organizations reduce costs because they do not have to install telephone lines or wiring. Cortes-Mendoza et al. (2017) explained cost-saving helps organizations to increase earnings offer higher flexibility and more features than a traditional telephone system. The success of an organization's VoIP systems depends on the price and quality of service.

Increased voice quality. The Quality of Service (QoS) measures the delayed traffic connections because of interference. Miraz et al. (2015) agreed that the range of jitters, end-to-end delay, and Mean Opinion Score occur because of the lack of QoS used to measure the VoIP traffic to the system. Mean Opinion Score has been used to measure the voice quality in the telephone network on a scale of one to five, with one being bad and five being excellent. Jitters are measured on arrival time in intervals of time, either underfilling or overfilling or both on the buffers of calls. End-to-end delay measures the number of packets it takes to transmit across a network from the source to its destination. Malisuwan et al. (2016) described that if the ranges are low, the QoS for real-time traffic for VoIP will be affected. Measuring the QoS of VoIP traffic will alert if the service is in trouble of being compromised. Ghalut et al. (2016) explained that many organizations categorize the effects of QoS into four areas service availability, service integrity, spam over internet telephony, and eavesdropping. With the increase in the VoIP system's reliability, it is essential to manage the QoS of VoIP traffic.

Negative Impact of VoIP. The negative impact of VoIP may occur with the use of a public IP network. Security of VoIP communication means securing confidentiality, integrity, and authentication of a VoIP connection. Ghalut et al. (2016) indicated that packet loss, jitters, eavesdropping, intercepting of voice communication, and latency contribute to negative performances of a VoIP network. Banerjee et al. (2018) described how a VoIP system requires security to secure voice and data networks to prevent unauthorized access from being compromised. A compromised VoIP network can make the receiver vulnerable to personal information stolen over the telephone lines. Sahin et al. (2017) agreed that VoIP fraud usually focuses on obtaining free telecommunication services or gaining financial benefits from its customers. VoIP victims are usually customers; employees subjected to fraudulent actives from interference.

Packet loss. VoIP packet loss occurs when messages from the communicator to the listener are not heard. Chen et al. (2016) noted that packet loss happens when many packets travel on a network that is not supported by the amount of VoIP traffic, causing the packets to get lost and the network to fail. Perkins and Singh (2017) detected that packet loss happens by observing a gap received in Real-Time Transport Protocol that increases latency congestion in a VoIP network. The resending of lost packets is impossible since all VoIP communication happens in real-time. Estepa et al. (2018) indicated that low packet loss must be maintained during communication to ensure acceptable speech quality. It is difficult to restore the communication between users once the discarded packets jitter.

Jitters. Jitters delay conversations between the two communicators allowing the call to sound like the communications are underwater. Khudhur et al. (2018) explained jitters are when the sender sends messages, and the receiver gets the messages slowly. Hephzibah and Oludare (2015) described that a VoIP network could determine if jitters are lost if a supported VoIP network is used to check VoIP sessions. When the bandwidth has lost time drifting, routing changes occur, making issues with the VoIP system. Alajmi et al. (2017) advised that each jitter packet takes time to go from one end to another without exceeding 20 to 50 milliseconds of jitters. VoIP applications use a buffer that can store some of the packets that are transformed into voice data.

Latency. The reason for latency delays could be many things such as distance, telephone devices, or the configuration of the network. Bensalah et al. (2017) insisted that latency delays a VoIP network with the time it takes for the voice to release from the phone and reach the listener. Ibrahim (2019) explained that packet delays are the crossing over of VoIP networks from a sender to a receiver. Also, Ibrahim explained that the call would drop 250 milliseconds after a network is delayed. The network will find the best possible path before dropping the call to reach the destination. Bensalah et al. found that latency is the end-to-end delay between sending and receiving packets that affect the IP network. VoIP networks should allow the best call packet to arrive at the receiver minimizing the chance for latency to begin.

Eavesdropping. Eavesdropping is another way for hackers to steal credentials from people conversing over the telephone. Satapathy and Livingston (2016) explained that eavesdropping allows hackers to obtain names, passwords, and numbers from conversations, which will give the hacker control over calls, billing, and voicemails. The hacker will eavesdrop to change the calling plans or control a victim's account. Cha et al. (2017) experimented that the quality of voice delays can cause eavesdropping and security issues using the distance between an original voice and a secured voice line demonstrating the severity of voice communication and eavesdropping. Dhar and Chatterjee (2017) found that hackers use eavesdropping to collect sensitive information to prepare for future attacks on organizations and their customers. Hackers secretly listening to phone calls without the consent of the communicators is a criminal offense.

Call spoofing. Call spoofing allows the caller to lie about their identity. Idom and Tormusa (2016) described that call spoofing is false names and numbers, so a caller can hide their identity so that it would appear on the phone or computer screen as a private call with the intention of fraud and or harassing people. Spoofing tricks people into answering the phone with a disguised caller ID. The customers who receive spoofing calls give their personal information to hackers whom they believe to be telemarketers. Hackers use the information to commit fraudulent activity. Eterovic-Soric et al. (2017)

insisted that hackers make nuisance phone calls using VoIP technology that allows users to spoof their outgoing phone number by bypassing the caller ID and number blocking. Tu et al. (2016) advised that the caller ID number could be spoofed because no built-in authentication mechanism can verify the recipient's phone number. Simmons (2016) explained the Caller ID Act; the Federal Communications Commission rules state that hackers that transmit inaccurate caller ID information are committing fraud. Customers of telecommunication organizations should be careful not to answer phone calls that are not identifiable to them as the call could be spoofed.

VoIP Security Concerns

There are several security concerns with both the organizations and the customers that use telecommunication organizations. The most severe is identity as a theft of service. This type of hacking is called phreaking, which steals services from a service provider while passing cost or credit card information to another person through VoIP calls (Jingi & Muhammad, 2017). The customer is vulnerable to getting their credit card and personal information stolen. Satapathy and Livingston (2016) described that eavesdropping is another way for hackers to steal credentials. The hacker will obtain names, passwords, and numbers from conversations, which will give the hacker control over calls, billing, and voicemails allowing the hacker to change the calling plans or take control over the victim's account. Hussain et al. (2015) suggested that DoS attacks on the network could be carried out on VoIP by targeting SIP call signals causing the calls to drop. Rajput and Barkatullah University Institute of Technology Bhopal, India (2017) explained that man-in-the-middle attacks is how hackers intercept call traffic and redirect the calls. On the other line, the victim will assume they speak with an organization requiring a bill pay and give their credit card information. The customer gives their personal and financial information to the hacker. Abouelmehdi et al. (2018) suggested that VoIP systems require security to secure voice and data networks to prevent unauthorized access. Securing a VoIP system will secure the customer and the organization from being compromised.

The main issue is that VoIP services used by telecommunication companies are not secured for the customers that use the services. Shaw and Sharma (2016) expressed that most organizations could not provide excellent VoIP services to satisfy their customers. A new security strategy should be implemented so that customers would not be afraid of speaking to a telecommunication organization. Abouelmehdi et al. (2018) insisted that the security measures for securing a VoIP system are maintaining, monitoring, filtering, authentication, and server design. Customers who reveal credit card and private information over the phone should not fear being compromised when speaking to a telemarketer. Sabillon et al. (2016) advised that attackers masquerade an organization's phone calls to gain either the customer or the organization to validate some financial transactions. The hackers who gain access to financial records use the information.

VoIP/Telecommunication Regulations

As more organizations adopt VoIP telephone systems, there seem to be more legal issues with the government. Gurrapu et al. (2016) described that the government wants regulatory fees paid, provided Emergency 911 (E911) services, and the allowance of government agencies to conduct surveillance. One example is the Federal Communication Commission, a regulatory agency that underlies the core provisions of telecommunication policies, oversees internet services, documents public utility for mass media and telecommunications. The FCC regulations require that all E911 calls be routed immediately, regardless of where the calls stem from (Van Noorden, 2016). Souppaya and Scarfone (2016) insisted E911 features had been problematic because subscribers to VoIP can change their Internet Service Providers network, making it challenging to find the subscriber's location. VoIP subscribers must have their current address when signing up for the service so that the E911 call centers can dispatch emergency personnel to their locations.

The FCC implanted a new law called the Telecommunication Act of 1996. President Bill Clinton signed the act that would change American Telecommunication law. Furchtgott-Roth (2017) suggested The Telecommunication Act 1996 represents the changes in American telecommunication organizations regulating telephone services local, long-distance, broadcast services, high-quality voice, data, and video technology. The law now included users of VoIP and Public Telephone Networks. Evens and Donders (2016) described the Telecommunication Act is to allow all telecommunication organizations to compete while creating fair rules. Therefore, the calling party would have to pay the called party’s carrier for completing the call. Brennan (2016) insisted that the FCC decided access charges should apply to VoIP providers to compensate for any lost revenues. VoIP providers don’t pay the same taxes as regular telephone providers, creating unfair conditions for VoIP services.

VoIP et Data Breaches in Telecommunication Organizations

VoIP had a data breach increase of 14 % over the past 2 years in telecommunication organizations (Velianitis al., 2018). Telecommunication organization has IT security managers that focus on lowering the security risk of their VoIP system. VoIP is a combination of applications that runs on the internet. Kolhar et al. (2017) agreed with Shaw and Sharma (2016) that users misuse VoIP protocols making it hard to secure a VoIP system. The amount of VoIP breaches remains high amongst telecommunication organizations. Rahman et al. (2017) found VoIP will be going through a full scale of implantations for the next year to achieve a system that cannot be hacked. VoIP protocols used on the internet for communication are not easy to secure.

Verizon is a telecommunication organization that has faced some VoIP telephone breaches. Tounsi and Rais (2018) indicated that Verizon uses a telecommunication service vendor authorized to provide and restore telecommunication services with Telecom Service Priority. Telecom Service Priority is a vendor authorized to provide and restore telecommunication services. Li et al. (2017) found that Verizon uses a crisis management team whose only objective is to manage and control all problems about a telephone network. The crisis team restores, recovers any lost data, and mitigates the situation. Shaffer (2017) noted that Verizon also gives tips on keeping your service secured by backing up data and managing the organization’s devices.

Relationship to Previous Research

Previous researchers have explained security issues with VoIP systems. Many researchers have found why a VoIP system would fail but never successfully addressed the problems. Fayyaz et al. (2016) found that at the beginning of VoIP, there was a lack of concerns and awareness about security. VoIP users were concerned about the quality and functions of VoIP when securing the network. VoIP security has become an issue as it becomes a communication technology widely used amongst organizations. Shaw and Sharma (2016) expressed that a telecommunication VoIP system should implement security measures on the internal network. Telephony over IP is established as a voice communication directly over IP networks allowing higher voice flexibility and cost-sharing of voice services. Previous research discussed by Alouneh et al. (2016) found that more security on VoIP communication may add more delays, packet loss, and jittering on the system. However, Hasan and Hussain (2017) previous research found that strengthening the network firewalls will reduce VoIP attacks. VoIP networks are at their best if they are maintained and monitored for interruptions.

The research strives to analyze the strategies to secure a VoIP telephone system. Hwang et al. (2019) found that VoIP is possible because the foundation uses the telephone and the internet. However, there have always been security issues with both technologies. Previous research noted by Kolhar et al. (2017) found many strategies to secure a VoIP system, such as port authentication, categorization of traffic, configuration authentication, authentication the signaling, and Encrypting the media. These methods were adopted because of previous research used to justify the security of a VoIP system. Ganesan and MSK (2017) focused on Session Initiation Protocol to secure a VoIP system because SIP uses values that authenticate messages that maintain confidentiality.

Securing a VoIP system seems complicated, especially when you have many different options for securing the network.

Transition

Section 1 includes the background of the problem, the problem statement, purpose statement; nature of the study; research question; interview questions; conceptual framework, operational definitions, assumptions, limitations, and delimitations; the study's significance academic literature review. This section includes RAT and its usage for securing a VoIP system. The IT problem is defined and focuses on the literature review to understand VoIP telephone systems. VoIP is widely used in telecommunication organizations and is a new, inexpensive, and beneficial technology to all organizations. However, the security aspect of VoIP poses a significant concern. Security strategies to control a VoIP telephone system from being compromised should help to reduce identity and credit card theft. Section 2 includes information on the role of the researcher, the participants chosen for the study; research method and design; the population selected; ethical research; the data collection instruments and techniques, and the reliability and validity of the study. Section 3 addresses the data collected and the findings of the study. Also, Section 3 highlights an overview of the study, presentation of the results, professional practices; implications for social change; a recommendation for action and further study; a reflection of the study; and the study’s conclusion.

Section 2: The Project

In this study, I investigated the strategies that IT security managers use in telecommunication organizations to secure a VoIP telephone system from intercepted and misused data. The following subsections include a discussion of (a) the purpose statement, (b) the role of the researcher, (c) participants, (d) research methodology, (e) research design, (f) population and sampling, (g) ethical research, (h) data collection, (i) data collection instruments and techniques, (j) data organization and analysis, (k) reliability and validity, and (l) data saturation.

Purpose Statement

The purpose of this qualitative, multiple case study was to explore the strategies that IT security managers in telecommunication organizations use to secure a VoIP telephone system from data being intercepted and misused. The population for this study was IT security managers employed by three telecommunication companies in New York that had strategies to secure a VoIP telephone system. The implications for positive social change include that the strategies may reduce identity and credit card theft from data breaches.

Role of the Researcher

My role as the researcher was to collect and analyze data from interview questions for this qualitative, multiple case study. The researcher focuses on all aspects of research design and data collection, such as creating an interview protocol (All et al., 2016; Ponelis, 2015). As the researcher, I was responsible for creating the interview questions, choosing the participants, and following a protocol to conduct ethical interviews. Using open-ended questions with the participants in the interview can lead to themes used later in the research (Ranney et al., 2015).

I used the same starting interview questions for all the participants. Fusch and Ness (2015) described that data saturation occurs when no new information is found and insisted some interviewers fail this objective because of not knowing how many interviews to conduct to satisfy saturation. Fusch and Ness also suggested data saturation might be hard to understand because it differs depending on the researcher or interviewer. Saturation grids are a method that includes essential topics and interviews conducted to ensure no further information is needed (Fusch & Ness, 2015). I created a list to document and ensure no new information exists after the interviews. Without reaching saturation, I would have recruited more organizations and participants if I got through the interview list.

I interviewed with a steady and calm tone, which allowed the participants to understand the questions. Additionally, I secured a relaxed and distraction-free location to facilitate the conversation. The participants were asked if they could be recorded, and the interview started when they agreed. After completion of the interview, I transcribed and analyzed the recorded information. Sutton and Austin (2015) suggested that a recording must be transcribed verbatim. It could take up to 8 hours to transcribe a 45-minute interview; therefore, I scheduled adequate time to ensure proper transcription. The interview questions focused on strategies used by IT security managers to secure VoIP communication within telecommunication organizations. Manzano (2016) suggested using semi structured interview questions to allow participants to clarify answers to any question. The participant was able to elaborate on the interview questions, which helped to ensure data saturation.

I protected the participant's responses by adhering to the three basic ethical principles of *The Belmont Report*, the standard for conducting ethical research, which are the person, beneficence, and justice (Bromley et al., 2015). The National Commission for Protection of Human Subjects in Biomedical and Behavioral Research (1979) created *The Belmont Report* to enhance the treatment of participants after abusive treatments performed by previous researchers. Bromley et al. (2015) described that respecting individuals revolves around protecting them and allowing them to be independent. The individual will be able to decide whether to participate in the interview process. Beneficence is securing the individual's well-being and informing the participant of any risks from the study (Bromley et al., 2015). Finally, Bromley et al. (2015) defined justice as that everyone is treated equally. I respected these principles by using the informed consent process to explain the participant's rights, further detailed in the Ethical Research subsection.

I currently reside in New York City, and I selected my research participants from at least three organizations located in the state of New York. There were no previous relationships between any of the participants and me. Before this study, I was not an expert in securing a VoIP system; therefore, I did not introduce bias because all information gained from this study was from data collection. As the sole person creating and conducting the interviews, I recorded, listened, and took written notes.

I have 20 plus years of experience in the IT field, which helped me understand the themes introduced by the IT security managers. Roulston and Shelton (2015) indicated that the researcher might have biases towards the research study since qualitative studies are subjective, and these biases can threaten the study. This type of bias is managed through the interview process by asking questions that can invoke bias from the interviewer (Roulston & Shelton, 2015). I decreased bias by recording the interviews and solely using the participants' responses to guide the research.

Participants

The population for this qualitative, multiple case study was IT security managers who worked for three telecommunication organizations located in New York that support a VoIP telephone system to conduct their daily business. The eligible participants had at least 2 years of experience securing a VoIP system from data being intercepted and misused and work for a telecommunication organization that uses a VoIP system. Berger (2015) suggested that a participant should know the field of study to answer the interviewer's questions. Additionally, Wolgemuth et al. (2015) indicated that the researcher should trust that the participant is truthful about the knowledge of the study. Dempsey et al. (2016) insisted it is vital for the researcher to reach out to a gatekeeper to send an email or letter to a the participant to request an interview. Then, the participant reviewed the consent, which gave them the right to refuse or withdraw from the study at any time. The interview questions were also provided to all the participants.

After receiving approval to conduct the study from the Walden University Institutional Review Board (IRB), I emailed an introduction letter introducing myself and the study to the possible participants. Wolgemuth et al. (2015) explained that introductions are essential so that the participant has a clear understanding of the study while also stressing the need to build a professional relationship. Establishing a professional relationship with the participant builds trust, allowing the participants to feel comfortable accepting the interview invitation. The participant will also then understand how their answers to the interview questions helped the study.

The interviewed participants received a consent form that notified them of what will occur in the interview. Arsel (2017) suggested that the consent form should let the participant know their rights, risks, and benefits as the study interviewees. Nusbaum et al. (2017) explained that the consent form protects a participant's privacy before any information exchanges between the participant and the interviewer. Tait and Voepel-Lewis (2015) indicated that the consent form reinforces for the participant that their signed authorization was a consent to participate. Finally, when the consent was signed, the participants were handed a copy of the consent form and were ready to begin the interview process.

I asked the open-ended interview questions, so the participant understood the questions entirely before answering. Castillo-Montoya (2016) insisted that the interview questions should align with the research questions so that the participant can understand their necessity for the study. The interviewer assists the participant by asking questions that will tell the participant's story while staying aligned with the purpose of the study. Castillo-Montoya (2016) suggested the interviewer should listen carefully to the participant responses when explaining their lived experiences. A researcher knows that careful listening is essential to understand the participant's experiences. Evans et al. (2017) noted that obtaining feedback and listening is how to conduct a great interview. The participants in the current study answered all the interview questions with ease. I ended each interview by ensuring the participant that all documents and tape recordings regarding the study would be saved for 5 years before being destroyed. All information will be kept confidential.

Research Method and Design

Exploring strategies IT security managers in telecommunication organizations use to secure a VoIP telephone system required a qualitative approach with a multiple case study design. The results of qualitative research describe the context of the study and the participants' lived experiences (Lewis, 2015). A multiple case study is used to observe participants and is well defined and structured (Yazan, 2015). A multiple case study design was appropriate for this study because it allowed me to describe the step-by-step strategies used to identify how telecommunication organizations secure their VoIP telephone systems.

Research Method

I chose a qualitative method to explore the strategies used to secure a VoIP system in telecommunication organizations. Qualitative researchers use this method to understand the research topic (Lewis, 2015). Percy et al. (2015) added that qualitative investigation includes data related to people's opinions, attitudes, beliefs, and reactions to their own lived experiences. The use of the qualitative method assisted me in gathering the IT security managers' experiences to answer the research question about the strategies used to secure a VoIP system. The qualitative method captures contextual details (Dey & Lehner, 2017).

In contrast, the quantitative method involves collecting numerical data to generalize information for the population; however, the available strategies in known research do not provide a basis for establishing external validity (Gorard, 2015). This issue presents a challenge in producing reliable variables. Instruments in the quantitative method (i.e., survey instruments) require a reliability test to ensure that participants can deliver information on the question asked without significant distortion (Heale & Twycross, 2015). This vital step helps deliver statistical information from a large sample (Kozleski, 2017). However, adequate research to form variables makes it difficult to create a reliable survey, so the quantitative method was not appropriate for this study.

I considered using a mixed-method approach for this study but decided against it because it combines qualitative and quantitative methods. Imran and Yusoff (2015) defined a mixed-method study as one that combines the strengths of both qualitative and quantitative methods to get accurate results when gathering data. Popping (2015) found that the collection of closed- and open-ended approaches is used to explore issues within the study. Furthermore, a mixed-method approach uses multiple rounds of data collection to gather both quantitative and qualitative data (Creswell & Creswell, 2017). However, the absence of quantitative variables made the use of the mixed-method approach not appropriate for the current study.

Research Design

I employed a multiple case study research design in this qualitative study. There were several research designs to choose from, but the two considered and not chosen were narrative and phenomenological designs. Percy et al. (2015) described a multiple case study as an in-depth investigation of multiple groups of people with data sources that define the case from many other instances. Additionally, a multiple case study involves collecting information from multiple sites, which delivers more insight into the phenomena (Salamzadeh et al., 2017). A multiple case study design was appropriate for this study because the data gathered from IT managers in telecommunication organizations helped to understand the strategies used to secure a VoIP system. I choose a multiple case study to investigate telecommunication locations to gain more information about IT security managers' strategies to secure VoIP telephone systems.

I considered the narrative design but did not select it for this study. Researchers use the narrative design to communicate a person's experience by telling their story (Elmes & Barry, 2017). Additionally, this design focuses on a three-step process to storytelling, including finding insight into the story, creating the story, and then telling it (Bryan et al., 2017). The narrative design also includes methods to communicate a wide range of sequences that supplies timelines with a smooth transition from one point of the story to another (Brehmer et al., 2017). However, the focus of this study was not a story of experiencing VoIP but gaining strategies that will secure it; therefore, I did not choose this design.

I also considered a phenomenological design. Hopkins et al. (2016) described a phenomenology design as one that is used to capture a human's lived experiences to explain or provide insight into a phenomenon. Interviews using this design often provide insight into how people appear and show themselves to a group of people in a lived experience (Hopkins et al., 2016; Van Manen, 2017). I did not choose this method because I was not looking to describe a phenomenon from lived experiences but rather gain common strategies used by IT security managers.

In the qualitative method, data saturation is reached by making sure the details of the study will not go unnoticed. Malterud et al. (2016) described data saturation as an ongoing analysis used to observe and compare similarities and differences in the research. When ensuring data saturation, there must be no new information found. Malterud et al. found that when data are being collected, the researcher must compare notes to exhaust all categories of the study. Therefore, to reach data saturation, I interviewed each participant with the same prepared research questions, documenting and recording the participant's answers. I then checked my notes to identify if any new themes were discussed. Malterud et al. stated that data saturation could occur only when the researcher has received no new information added to the study. I conducted interviews until no new information was found and data saturation was reached.

Population and Sampling

The population for this study was IT security managers from at least three telecommunication organizations in New York. They have experience in the strategies used to secure a VoIP telephone system. Gentles et al. (2015) suggested that population selection should reflect the purpose of the research topic. The researcher chooses the participants who have the characteristics to join the study (Nebeker et al., 2016). The requirements include (a) IT security managers, (b) 2 years' experience in securing a VoIP telephone system, (c) working for a telecommunication organization in New York. Thomas (2017) suggested selecting participants willing to share their experiences. All the participants met the criteria to participate in the study.

I contacted telecommunication organizations located in New York to engage in the study. Dusek et al. (2015) insisted that total population sampling involves examining the entire population with a set of experiences, knowledge, or skills about the research questions. I contacted the gatekeeper of the telecommunication organizations by sending an email alerting the person or persons reading the letter that I was looking for participants to participate in the study titled the strategies used to secure a VoIP telephone system. The gatekeeper is the point person to connect with to get the approval to conduct an interview (Marland & Esselment, 2018). McGuirk and O'Neill (2016) described that when sending a letter to your population, the letter should include purposeful information about the study, confidentiality, length of the interview, participants for the study. In the letter to my participants, I included any doubts that the participant may have.

Purposive sampling was used to select participants for this study. Etikan et al. (2016) explained that the researcher used purposive sampling in qualitative studies to locate participants willing to share information about their knowledge or known experiences about the research. Purposive sampling was used to gather information from the participants to understand how IT security managers secure a VoIP telephone system from data being intercepted and misused. Ebersole et al. (2016) indicated that with the nonrandom selection of participants, the researcher impedes the ability to be biased against the participants. The researcher expects each participant to provide information that will be of value to this research. Etikan et al. found the weakness of purposive sampling is to be strict at including the participants' interests and not include those that do not suit the full purpose of the research. This weakness means that I had to select IT security managers who secure VoIP but exclude any who only had one of these criteria. Palinkas et al. (2015) emphasized that purposive sampling methods obtain saturation by sampling until no new information is acquired. The nine chosen participants have the experiences and knowledge to share information to help the researcher reach data saturation. All participants were asked the same beginning interview questions. After the interview process, the researcher listened to the recording and determined if any new information was needed.

Total population is a method of purposive sampling used for this study. Etikan (2017) described total population sampling is a technique where the criteria meet the skill set in the research being conducted. Total population sampling was useful because it gave me the information needed from the IT security managers currently securing a VoIP system, which provided conclusive results for the research. Gentles et al. (2016) explained the power of Total population is that the interviewees are knowledgeable about a subject area and are willing to share their knowledge. I interviewed IT security managers who are experts in their fields that work for telecommunication organizations in New York.

Total population sampling allows all the IT security managers to participate in the study. The sample size for qualitative research depends on the number of participants needed for the study (Thomas, 2017). I reached data saturation when no new information was presented on the topic. Malterud et al. (2016) indicated a small sample size for qualitative research should be sufficient to address the research question. While Thomas (2017) mentioned using a large sample size can lead to repetitive information. Therefore, I will select three telecommunication organizations to participate in this study. For this qualitative multiple case study, the sample population was nine IT security managers securing a VoIP telephone system three IT security managers from each telecommunication organization in New York.

Ethical Research

I used the informed consent process to ensure ethical protection for participants and the organization during this study. Giorgini et al. (2015) explained that ethical guidelines are established to create a consistent normative standard for researchers in their fields and to avoid the legal consequences of ethical breaches. I used the consent process, which informed the participants of their rights to participate in the study. Also, participants were informed that there were no incentives for participating in the study. Vitak et al. (2016) suggested using practices recommended with the institution's Institutional Review Board to conduct responsible research. The study was moved into the data collection phase only when the IRB approval # 05-22-20-0189185 from Walden University approved the ethical safeguards for human participants.

Ethical consideration training requirements were met when I completed a training course Protecting Human Research and received a certificate (Certificate Number: 1952722) given by the National Institutes of Health (see Appendix). This training was done to understand the background for The Belmont Report and 45 CFR 46. Each concept will be considered during the design of the data collection phase. For example, keeping the participant anonymous and requiring permission to use direct quotes that might attribute to them (Algozzine & Hancock, 2016). The participants and their organizations were deidentified by using codes. Participants are labeled by P and a. number, while the organization uses O and a number. For instance, the first participant is P1O1, while another from the same organization is P102. I informed the participants about the informed consent process and ensured the participants of their rights, benefits, and risk of the study.

Additionally, I informed the participants that all shared information with the researcher is confidential. Finally, the participant had the right the refuse or withdrew from the study at any time without notice. If the participant withdraws from the study, I will store the data on an encrypted flash drive locked in a combination safe for 5 years.

Participants will receive a copy of the informed consent process for their records. Kass et al. (2015) noted that written consent signifies the assumption that the participants understand all the information provided to them. I ensured the importance of reviewing the informed consent process to understand their rights to confidentiality and security and did not conduct any interviews unless the participant signed their agreement. Tucker et al. (2016) insisted that researchers keep the data safe to protect the participants and organizations. Data for this study will remain stored on an encrypted flash drive and locked in a combination safe for 5 years. Colp et al. (2015) suggested that an encrypted storage device protects sensitive information, such as participants' answers. The flash drive with the researched data will have a password with a PIN that can only be accessible by me.

Data Collection

Data collection was conducted via interviews and document reviews for this qualitative multiple case study. The semi-structured interviews will consist of open-ended questions that IT security managers connected to telecommunication organizations in New York will answer. I used an organization’s gatekeeper to locate and communicate with qualified participants. The interviewed responses were recorded, noted, transcribed, member checked, and collected as data for the research. The interviews helped in the data collection process by gathering the information needed from IT security managers on the strategies used to secure a VoIP system in telecommunication organizations.

Data Collection Instruments

I am the data collection instrument and obtained information using semi-structured interviews with open-ended interview questions for the participants. McIntosh and Morse (2015) described the semi-structured method allows the interview questions to focus on the participants' responses so the researcher can probe asking for clarification. Additionally, Kallio et al. (2016) insisted that this form of questioning prepares the researcher to investigate details on the topic. I used this method to gain in-depth insight into each question by clarifying any information provided by the participants. As the sole data collector, I asked four types of open-ended interview questions. Castillo-Montoya (2016) insisted on reaching the conversational and inquiry goals of the research in an interview. One should include the four types of questions (1) preliminary questions, (2) transition questions, (3) key questions, and (4) closing questions. The interviewer should keep the participant engaged in the interview process until all questions are answered.

My goal is to ensure that the participants are comfortable and accurately capture all the data. Hogan et al. (2016) suggested getting an in-depth insight into the participant's experience should remain the researcher's primary goal. A digital recorder was present to record the participants with their permission, while a notebook to take field notes enhanced the understanding during analysis. Oltmann (2016) advised professional attire and refraining from any nonverbal body language and mannerisms that can lead to misinterpretation. I conducted myself professionally and gained the rapport of the participants for a productive interview. Dempsey et al. (2016) reminded that the interviewer should know how long the interview will be before entering the interview. I respected my participant's schedules by reminding them of allotted time before entering the interview and signaling when the time was close to completion.

When the interview began, I reminded the participant of the time and their rights to refuse and withdraw from participating in the study. I asked the participant if they were comfortable and ready to start recording. I asked the participant for their consent form, naming them as participants 1, 2, 3, and the organization as organization 1, 2, 3. I began asking the research questions to the participant and adding additional questions based on the participants' responses. The interviews lasted approximately 1 hour.

After the interview, I explained transcription and the member-checking process to the participant. Sutton and Austin (2015) suggested transcribing interviews before analysis so that the researcher can run an analysis for written text for common themes. Analyzing the written text allows the researcher to code and categorize linked words or phrases. Ibrahim and Edgley (2015) indicated that the researcher should check for underlying themes when transcribing, making sure that the developed themes are accurately represented in the data. The detailed analysis method allowed me to identify if additional research is needed. Erlingsson and Brysiewicz (2017) emphasized that it is essential to understand the study to avoid bias during the member checking process. When analyzing the data, bias was limited, and the transcription was used to confirm the interpretation of the participant’s words.

Member checking is used to increase the study's trustworthiness and validate that data saturation has been reached. Member checking verifies that the interpreted statements from the participants are accurately interpreted (Birt et al., 2016). I asked for a second interview either through Zoom or a phone call so the participant could validate or correct my interpretation of the data. Thomas (2017) suggested that member checking will validate the reliability of the data results, which is reached by both the researcher and the participant. Using member checking helped limit my bias by using the participant’s experience to gather information on the strategies to secure a VoIP telephone system. Amankwaa (2016) indicated that member checking reduces bias by allowing the participants to confirm the data results. Member checking of the collected data occurred when the researcher shared the interpreted data with the participant’s responses to ensure that the data provided is accurate and understood between the participant and the researcher.

Data Collection Technique

The data collection techniques for this qualitative multiple case study were the use of open-ended interview questions, focusing, note-taking, allowed document reviews, organizational documents, voice recordings, transcribing, and member checking. Petrie (2016) suggested that the interview process is the most powerful tool in a qualitative study, as interviewing helps collect data from participants' experiences. The data collected was sorted and characterized so that when transcribing and member checking takes place, the correct information comes from the correct participant and their organization. Oh et al. (2016) described that the interview process is a big part of collecting data, so the researcher must be effective in the interview process when collecting data from the participant. The main objective of collecting data is to answer the research question. The researcher must first gain the participant’s trust. The researcher should assure the participant that the information used is solely for the research and nothing else. Jagosh et al. (2015) theorized that building and maintaining a trusting relationship with the participant would allow the trusting relationship to grow over some time. When collecting data in an interview setting, the researcher's primary focus is gathering data and a trusting relationship with the participant.

Data collection techniques started by handing a consent form to the participant to permit the researcher to record, conduct, transcribe, and member check the interviews. Kallio et al. (2016) confirmed that semi structured interviews are a common way to collect data in a qualitative study adding quality to the research results. The researcher asked the participant if a recorder could be used in the interview. Oltmann (2016) insisted that using a tape recorder in an interview setting is necessary for capturing the progress of the interview. Before beginning the interview, the researcher thanked the participant for agreeing to meet. Heidt et al. (2016) suggested that thanking the participant before and after the interview is essential for the participant's generous consent to participate in the study. The researcher reminded the participant that the recording and the interview could be stopped at any time.

I explained to the participant the focus of the interview, which is to address the research question in the study. Castillo-Montoya (2016) indicated that research questions should be spoken to understand. The researcher started the recorder and began to conduct the interview naming the participants and their organizations in numerical order as to when the interview took place. Example: Participant 1 = P1, and Organization 1 = O1 etc. Allen and Wiles (2016) suggested that the renaming of participants in research studies has meaning to both the researcher and the study, keeping the participant anonymous and organized. When the interviews started, the researcher began reading the open-ended interview questions steadily, ensuring that the participant understood the interview questions. Arsel (2017) insisted that speaking concisely and clearly during the interview will allow for the interview to flow. After each question, I will give the participant time to respond completely before asking the next question. Using the open-ended question method, the researcher can, and should, ask additional, probing questions after hearing the participant's response.

When ending the interview, I thanked the participant and explained the next steps to the participant. Alase (2017) suggested the recorded interview be transcribed, and the interpretation of the participant responses be typed for the participant to review. A second interview was required either by Skype or Zoom for the participant to member check the accuracy of the interpretation from the interview. Madill and Sullivan (2018) indicated that member checking takes place in the fourth stage of the interview process, which is an informal post interview where the participant is given a chance to discuss and approve the accuracy of the interview. I double-checked the information to the feedback from the participants and confirmed that the interpretation explains the participant's experiences. Varpio et al. (2016) explained that member checking is a respondent validation that enhances the credibility of the data analysis and the participant's involvement. Using data collection techniques increases the credibility, the truthfulness of the study and represents the participant's experiences. I securely stores the data to protect the research.

Data Organization

Data organization techniques are essential for researchers to stay organized. Moore and Llompart (2017) explained that data organization is helpful for researchers to collect, analyze, and manage data. Researchers should securely keep all documents included in the study, such as interviews, consent forms, and written documents.

Data organization of interview questions will be labeled as participants 1, 2, 3, and organization 1, 2, 3, etc. The transcribed interviews were written in a Microsoft Word document. The documents will be saved and stored on a flash drive protected with a four-digit pin for 5 years. Castillo-Montoya (2016) suggested that organizing your interview question will promote a conversational flow. The researcher has organized the interview question to flow, allowing the participant to answer each question freely. Any questions that arise after the participant answers the participant's initial question is allowed to answer. Kallio et al. (2016) explained that focusing on important issues will keep the participant interested in the interview. The participant's responses are organized in order and typed in a labeled Word document interview 1, 2, 3, etc. For the participant to member check in a second interview. Birt et al. (2016) found that member checking is known as a participant's validation, where the trustworthiness of the transcribed data is viewed for clarity. The data organization of the interview includes storing all collected data on a flash drive with an encrypted password that is in a combination safe for 5 years.

Data Analysis

The data analysis process involves data collected from semi structured interview answers, note-taking, and themes formed before and after the interview process. The analyzed data answers my research question regarding the strategies IT security managers use in telecommunication organizations to secure a VoIP telephone system from intercepted and misused data. A qualitative analysis process involves coding and sorting data into themes and categories carefully examined and compared by the researcher (Mason, 2017). I carefully analyze all the interviewees' notes and interview answers related to securing a VoIP telephone system in telecommunication organizations. Analyzing the data allows the researcher to describe the themes and concepts of the received data (Neale, 2016). The collected data enables the researcher to fully explain IT security managers' strategies to secure a VoIP telephone system in telecommunication organizations. The analyzed data allows the researcher to see the frequent codes, categories, and themes throughout the data, capturing the essential relationships to the overall research question (Vaismoradi et al., 2016). When analyzing the data, I used the research questions and themes to focus solely on IT security managers' strategies to secure a VoIP system.

To increase validity and to strengthen the study, I used triangulation. Data triangulation is used in qualitative research to understand an experience by using multiple sources of data (Joslin & Müller, 2016). I used data triangulation to enhance the credibility of the research by using multiple ways of collecting data to answer the research question. When collecting data from multiple sources such as interviews, document reviews, and note-taking, triangulation and saturation will occur when enough data has been collected, and no new data is surfacing. Data triangulation joined evidence from interviews and written documents for the study's findings (Varpio et al., 2016). Triangulation of data aids in reducing the potential for bias by using responses from multiple sources to include in the study. Hadi and Closs (2016) acknowledged that data triangulation confirms the credibility, reliability, and validity of the data in the study. In the data analysis phase, data triangulation is beneficial because it enhances the confirmation of the data. Olson et al. (2016) indicated that the overall validity of the research study is gauged using data triangulation to contribute to the trustworthiness of the study. Using the data triangulation method helped analyze the data from notetaking, interviews, documents, and themes in the study.

Some steps are followed in the data analysis phase to determine the problem and answer the research question. Emmert-Streib et al. (2016) found that the sequence for data analysis is an overall assessment of the problem. Coding the data should help to categorize the data and develop themes. Gaur and Kumar (2018) indicated coding scheme generates confidence in the analyzed content. Coding defines the data and finds relations that will identify similar text. I listed all the collected data by participant number, organization number, and dates. The themes were categorized into similarities, differences, causes, and effects of IT security managers' strategies in securing a VoIP system. Moore and Llompart (2017) suggested making a spreadsheet that lists the coded text from the collected data. I organized the information provided using coded themes and added it to Dedoose and Microsoft Word software to determine the final data analysis.

I have chosen to use Microsoft Excel, Word, and Dedoose to code and identify themes. Bree and Gallagher (2016) suggested using Microsoft Excel for analyzing qualitative data for identifying, analyzing, and reporting patterns within the data. Ose (2016) explained that Microsoft Word is needed to structure text into main categories, topics, and subtopics, making it easier to read through the text. When transcribing the participant’s experiences, I used Microsoft Word. Ose corroborated with Bree and Gallagher that Microsoft Word is excellent for structuring data if you follow these steps:

1. Collect the data.
2. Transcribe the audio files.
3. Transfer the text from Excel to Word.

4. Transfer quotes and references from Microsoft Word to Dedoose.
5. Sort the text into a logical structure based on the coding.
6. Analyze the data into themes.

I typed up the transcribed information from the interviews into Word, and then I used Dedoose to find the themes needed to ensure that I had reached data saturation.

Dedoose helps with analyzing qualitative research with text from spreadsheet data. Zhao et al. (2016) suggested that Dedoose is a user-friendly interface that creates a virtual shared workspace that stores, manages, shares, analyzes, and organizes an increasing amount of collected research data. Dedoose was used to code the data for this qualitative case study. Adu (2019) indicated that Dedoose would generate an outline to categorize the chosen categories' themes and subthemes. I found common, transcribed themes. Drouhard et al. (2017) described that Dedoose correlates the visualizations of code distribution and analyses the data. I used REV to transcribe the interview experiences into a Microsoft Word spreadsheet. Then I uploaded the transcription to Dedoose to find the common themes to ensure that I had reached data saturation.

Reliability and Validity

Quantitative studies use statistical tests to measure reliability and validity. The equivalent of the qualitative methodology involves enhancing the study's trustworthiness. To enhance the trustworthiness of this study, I ensured that the research was reliable and accurate. Dikko (2016) suggested that for research to be considered credible, it must pass the test of validity and reliability. For this qualitative research study, the strategies used to provide reliability and validity are dependability, credibility, transferability, and confirmability to validate that this research is credible, as described below.

Dependability

Dependability was used to demonstrate the trustworthy information of the research findings. Kabir (2017) explained that dependability provides the consistency and strength of the research study. In this study, dependability was achieved using the interview protocol with all the participants, member checking to ensure that the data collected is accurate. Dependability must be consistent feedback from the participant's interview answers to ensure trustworthiness in qualitative research (Laumann, 2018). I used my notes to address concerns and Dedoose to identify the themes to verify consistency in the study findings. Dependability enhances the credibility of data analysis and participant involvement (Varpio et al., 2016). I achieve dependability in this research study by using triangulation, member checking, Microsoft Word, and Dedoose to achieve accuracy in the research findings.

Credibility

Credibility is a scientific standard for the quality of evidence needed in research (Vazire, 2018). The quality of data collected came from gathering multiple data sources using triangulation to make sure information is not missed. The data gathered are from participants that work in telecommunication organizations and know the strategies used to secure a VoIP telephone system. Bengtsson (2016) considered that establishing credibility happens when analyzing data to ensure no relevant data is excluded. Having the participants review the transcribed data and give feedback to any changes has credited the study. Stewart et al. (2017) emphasized that researchers should be trusted to produce reliable data that is credible and trustworthy in qualitative research through the adherence of evidence. For this qualitative case study, member checking was used to interpret the participants' experiences, adding credibility to all the data collected from interviews and note-taking.

Transferability

Transferability is used to obtain the external part of validity that brings worth to the study by requiring the researcher to give details about the study, such as people and experiences, to make the study understandable to the reader (Hadi & Closs, 2016). Eligible participants were carefully chosen, and the consent form gives a list of the participants for the study. Korstjens and Moser (2017) indicated that transferability is the researcher's responsibility to provide an in-depth description of the steps that lead to the research process, enabling the reader to determine if the study's findings are transferable. I read the same 12 interview questions to all the participants in the same order transcribing the data and member checking. Wu et al. (2016) insisted that the research should have contextual features common in the study samples to deem a study transferable. As the researcher, I transparently describe the research step by step, achieving credibility, transferability, and confirmability throughout the whole study by using triangulation and member checking.

Confirmability

Confirmability establishes that my interpretations are clear from demonstrating a conclusion from the data collected (Nowell et al., 2017). I did not have an opinion on the interviewed participant's data to the researcher. Kalu (2017) agreed to ensure the confirmability of the study's detailed data that all information should come from the participant. Obtaining confirmability for this qualitative case study, I addressed that the participant confirmed that the information collected in the interviews is the participant's experiences during the member checking process. Brown et al. (2017) indicated that judging the study's soundness is to document the participant's findings. I established confirmability by taking notes, transcribing, and member checking to ensure that the data collected is from the participant's experiences.

Data Saturation

I used semi-structured interviews and notes to analyze the data received to achieve data saturation. Saunders et al. (2017) described data saturation as being used in qualitative research as a criterion for discontinuing data collection or analysis. This research study achieved data saturation when no new data had surfed in the data collection process. Tran et al. (2016) suggested that for data saturation to be reached, probing needs to continue until the researcher feels they reached data saturation by fully understanding the participant's perspective of their experiences. I used open-ended interview questions from IT security managers; their responses let me know if I had reached data saturation when I analyzed all the data collected. Kim et al. (2016) found that the failure to reach data saturation would impact the quality of the conducted research. I continued to interview participants until data saturation was reached, and no new data were found. I knew when data saturation was achieved when no new themes emerged in the study.

Transition and Summary

Section 2 includes the purpose statement, the role of the researcher, the participants, ethical research, data collection techniques, and analysis, reliability, and data saturation. This section provides the process for conducting a qualitative case study on the security strategies used by IT security managers in telecommunication organizations to secure a VoIP telephone system from data being intercepted and misused. The data was gathered from the semi-structured interview responses and note-taking to achieve the strategies used in securing a VoIP system. Section 3 addresses the data collected, the study's findings, an overview of the study, presentation of the findings; professional practices; implications for social change; a recommendation for action and further study; a reflection, and a study conclusion.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

The purpose of this qualitative, multiple case study was to explore the strategies that IT security managers in telecommunication organizations use to secure a VoIP telephone system from being intercepted and misused. Kim et al. (2015) that 25% of VoIP telecommunication organizations reported unauthorized access to their customers' personal information. Malik and Choudhury (2019) also stated that telecommunication organizations enable call dialing to prevent criminal attacks on their telephone system. Azad et al. (2018) indicated that securing a VoIP telephone system has been challenging due to many fraud levels. IT security managers that work to protect VoIP telephone systems in telecommunication organizations could use the findings of this study to reduce the rate of telephone fraud.

I used the RAT as the conceptual framework of this study. Semi-structured interviews, consisting of 12 open-ended interview questions, were conducted with nine IT security managers from three telecommunication organizations in New York to address the following research question: What strategies do IT security managers use to secure a VoIP telephone system from telecommunication organizations intercepted and misused data?

I used Dedoose to find themes and subthemes within the data from the interview transcripts. This software contributes to qualitative scholarly work because Dedoose assisted in coding and examining patterns (Garth et al., 2017). I identified four themes representing IT security managers’ strategies for securing a VoIP telephone system in telecommunication organizations:

1. Best practices for VoIP security.
2. Using a secure VoIP provider.
3. Following VoIP security recommendations.
4. Awareness of future security concerns.

Presentation of the Findings

The participants in this study were IT security managers who had experience securing a VoIP telephone system. The role of an IT security manager includes securing and maintaining the VoIP telephone system from unauthorized users. I initially asked 12 IT security managers to participate in this study. While I wanted four from each of the three cases (i.e., telecommunication organizations), only nine IT security managers agreed to be interviewed. All the interviewed participants had over 2 years of experience securing a VoIP telephone system in telecommunication organizations. I numbered the interviewees as participants 1 through 3 and the organizations as O1 through O3. This identification method means that Participant 3O2 is Participant 3 from Organization 2. After interviewing the sixth participant, I reached data saturation because I did not identify new themes or codes with the seventh through the ninth participants. The ninth participant also provided me with an organizational document.

Four major themes emerged from the semi structured interview responses of IT security managers about the strategies they used to secure a VoIP telephone system. From the four emergent themes, subthemes also emerged that indicated why securing a VoIP system is essential to organizations.

Theme 1: Best Practices for VoIP Security

All participants' first theme was the best practices for securing a VoIP telephone system. The findings show how these precautions helped protect a VoIP system in securing telecommunication organizations. The participants mentioned the following three subthemes:

- VoIP security monitoring.
- Secure user credentials.
- Security patches.

The participants stated that these three subthemes must secure a VoIP telephone system and keep the system from failing. Table 1 shows the participant data that suggested the three subthemes related to the theme of the best practices to secure a VoIP telephone system.

Table 1

First Major Theme: Best Practices for VoIP Security

Subthemes	VoIP Security Monitoring (d)	Secure User Credentials(d)	Security Patches (d)
Participants	9	9	9
Documents	1	1	1

Note. d = data collected.

VoIP Security Monitoring

One crucial point discussed by all participants is to use security monitoring when securing a VoIP system. Compliance, software, and end-to-end encryption are VoIP security monitoring strategies and are the first steps to securing a VoIP system. Security monitoring, when used as a security strategy by IT security managers, may keep VoIP systems from being compromised. The compliance process ensures that external and internal design complies with the company's policies. Participant 3O1 indicated that security monitoring starts with knowing the organization's compliance policies, which supports Gavilanez et al. (2017), who stated that safely managing the configuration of a VoIP system to integrate security management for compliance policy should ensure risk management.

Participant 2O2 indicated that VoIP security monitoring starts with the transport layer security, a cryptographic technology protocol that encrypts data transfer over the internet. Mazhar and Shafiq (2018) explained this network management technique implements QoS to prioritize VoIP by encrypting the transfer flow to the network. Participant 2O3 also uses a compliance policy to record and track any abnormal activity in the system, preventing any VoIP breaches from taking place on the network. Siniarski et al.'s (2017) findings support all the participants' responses to having a VoIP monitoring system in place shields the VoIP from unapproved access by unwanted users.

All participants indicated they use VoIP software, which allows voice and data transmission over the internet, call reporting capabilities, and support functions, such as conferencing and messaging. Gandotra and Perigo's (2020) findings support that using support software enhances VoIP call registration and call routing capabilities. The participants all stated that they used software to manage a VoIP system within their organizations. Participants 1O1, 1O2, and 1O3 indicated that their organization uses a VoIP service provider that provides Verizon, Vonage, and Cisco software. Ali et al. (2020) suggested that the Verizon software identifies and analyzes recurring toll fraud trends or phishing calls. Verizon monitors and manages its infrastructures 24 hours a day. Fatehi and Choi's (2018) showed that Vonage is cheaper and competes with any other provider to allow the organization to switch, providing service quality, prices, and convenience. Many organizations will go with Vonage because it is cheaper and more convenient to switch to a new provider. Airi and Anderson (2017) reported that Cisco software helps control the VoIP telephone system's vulnerability. These three VoIP service providers aid in protecting a VoIP system from having data intercepted. Participant 2O1 said they use key performance indicators (KPIs) to maintain the VoIP system. KPIs are used to measure successful performance and the QoS (Muelas et al., 2017). For example, a KPI can describe the situation as critical when the organization knows that a carrier is completely down and cannot complete the call. A hotspot on the organization dashboard sends alarms to the monitoring team.

All the participants insisted that end-to-end encryption is needed to secure data the sender is not sending. End-to-end encryption happens when people want to read or listen to encrypted content, protecting against eavesdropping (Ntantogian et al., 2019). Participant 3O3 shared the following experience: "a man-in-the-middle attack was prevented due to end-to-end encryption intended to stop voice calls from being heard." Kfoury and Khoury (2018) confirmed that end-to-end encryption between VoIP users can be critical because it stops malicious behavior between end-users and stops them from listening to unauthorized conversations. End-to-end encryption prevents access to the VoIP system with the idea of addressing an attack before it happens.

This subtheme of VoIP security monitoring is supported in the literature. Monitoring a VoIP security system in telecommunication organizations is necessary to minimize the risk of attacks, interception, and the misuse of privately communicated information over a VoIP telephone system. Nuño et al. (2020**)** suggested that call monitoring collects data from the VoIP calls to activate security countermeasures to redirect the calls to the correct location. All the participants were adamant that VoIP security monitoring is needed to secure a VoIP telephone system. McInnes and Wills (2021) stated that the overall goal of a monitoring system is not to allow the telephone system to get infected by hack attempts. Any organization with a security monitoring system in place reduces the risk of being susceptible to the invasion of their information. Securing a monitoring system is recommended by Akinbami et al. (2018) and Satapathy and Livingston (2016), who insisted that monitoring a VoIP telephone system is essential to protecting an organization's private information.

This subtheme aligns with the conceptual framework of the RAT. Reyns et al. (2015) suggested that the RAT is used to determine why the criminal activity is taking place and try to control the crime from happening, which aligns with the actions that IT security managers take to ensure an organization's VoIP system is secured. The RAT is comprised of the three parts for a crime to occur: a motivated offender (i.e., hacker), a suitable target (i.e., customers), and a guardian (i.e., IT security manager who can secure the VoIP system from being compromised). Leukfeldt and Yar (2016) confirmed that offenders will not attack a suitable target with the guardian present who monitors routine activities. The current study results are consistent with Hawdon et al. (2019), who confirmed the likelihood of experiencing cyber violence and becoming a victim because of an online routine such as talking on the telephone. The subtheme of VoIP security monitoring aligns with the theme best practice for VoIP security to alert IT security managers when a VoIP crime is taking place and control the crime before it becomes serious.

Secure User Credentials

A secure user credential is a username and password created and used by only one user (CITE). An IT security manager can create a username that is specific to a person's name or identity and can identify a person using the system. Nuño et al. (2020**)** defined secure credentials as controls that allow access to specific resources. Using secure credentials is crucial for VoIP. For example, Dhillon and Kalra (2019) emphasized the importance of ensuring that a user's credentials are secured so that data are not compromised. All participants agreed with Naeem et al. (2020) about having no more than two authorized people with credentials and access to the VoIP system. The participants suggested keeping track of who has access to the system is essential to identify who has accessed the service reports generated by the network. Participants 1O2 and 2O3 explained the importance of securing credentials to protect the systems from being compromised. Saidat's (2019) agreed that having a secured credential is essential for monitoring and securing a VoIP system.

A secure and robust password can protect from intruders. Payne and Abegaz (2017) indicated that a hacker could hack into a VoIP system and gain access to a password that is not secured. Participant 3O3 gave an example of what could happen when a VoIP system is compromised because of a password. The participant stated some VoIP devices come with preset passwords. When a business resets its phone from the factory setting, the first thing to change is the password as soon as possible. Valente and Cardenas (2017) confirmed that VoIP devices have preset passwords publicly available on the internet, allowing hackers to bombard the interface with unlimited passwords of 16 keys to encrypt the VoIP traffic. Participant 2O3 suggested using a password combination of symbols and numbers when composing a solid password. The participant's experiences are supported by Johnson et al.'s (2019) finding that creating password data sets containing numbers in the 10s or 100s blocks hackers from gaining access to password information. All nine participants suggest never using the same passwords twice or using your name or birth date in any part of the password.

IT security managers use authentication to secure a VoIP telephone system. Jingi and Muhammad (2017) defined authentication as a strategy to identify a user's identity, preventing unwanted access to a VoIP system. Participant 1O1 explained the standard authentication method used to avoid unauthorized access is to have user and password verifications that the user only knows. Jan and Qayum (2017) shared that authentication protocols offer security guarantees that satisfy a VoIP system's performance and scalability. Chaudhry et al. (2017) also supported authentication to secure messages from clients containing secret information. Authentication provides security against unauthorized access by internal and external attackers. Participant 2O2 explained that everyone on his team receives a four-digit access code to see who has access, makes changes, or runs reports on the VoIP system.

This subtheme, secured credentials, is supported in the literature because IT security managers should use secured credentials when accessing and identifying themselves utilizing a VoIP system. Semerci et al. (2018) indicated that permitting users to log in to access the VoIP system will help them know who has gained access to the VoIP system. Depending on the layer of access, the user can control and perform the needed task. According to what the organization needs viewing VoIP call logs, access permissions are granted to a few selected people (Packer & Reuschel, 2018). According to Li et al. (2018), call logs consist of incoming and outgoing calls on the VoIP system. Harnack and Talbot (2017) agreed that call records give an organization a lot of information to analyze if the VoIP system is operating sufficiently or is compromised; this helps by recognizing numbers, names, call times, dates, and the duration of the call. Therefore, the findings show that using a secured credential is essential to secure a VoIP system from unwanted users.

This subtheme, secured credentials, aligns with the RAT framework because IT security managers must assign secured credentials to use a VoIP system. It is also vital for an IT security manager to ensure a VoIP system is secured before it becomes compromised because of a user's credentials. RAT endorses the purpose of this study of securing a user's credentials and ensuring that IT security managers grant the permissions needed to the organization's VoIP system (Makhdoom et al., 2019). The secure user credential theme is consistent with the RAT theory and supports the findings, this study's purpose, and the research question. All participants ensured that they used secured user credentials to prevent hackers from gaining access to the organization's VoIP system. The one document obtained focused on VoIP procedures that enforced passwords and authorization on voice calls to minimize eavesdropping and unauthorized access to a VoIP system (Araneo et al., 2018). This research and previous research support these findings of many organizations and the access to their VoIP system. The subtheme secure user credentials align with the theme best practice for VoIP security. IT security managers should take measures to secure a VoIP system, and giving workers secured credentials will help IT security managers identify who is using the VoIP system.

Security Patches

Security patches are essential because they look for common VoIP problems and fix them before they become urgent. For example, Jingi and Muhammad (2017) identified security patches for VoIP as vulnerabilities and countermeasures that can take place on a VoIP network. Participant 3O2 suggested running security patches at least once a month to secure a VoIP network. Geneiatakis et al. (2018) supported the participant's experiences, agreeing that IT security managers should not install a VoIP system without security risks. This research proves that a VoIP system inherits all vulnerabilities when deployed on the same IP network. Quamara and Gupta (2018) concurred that an IP network component consists of devices like routers, firewalls, and switches introducing vulnerabilities. The participants suggested paying close attention to the VoIP network's threats will secure the VoIP system.

A VoIP router log records the calls that come through to the organization's VoIP phone system. Oo and De La Salle University, Manila (2019) confirmed that a VoIP router log could check authorized IP blocks and ports. The routers accept the actual IP address and ports and deny any other IP address access. Participant 1O3 explained that router logs are emailed every week, but text messages and email alerts are sent if there are problems. The issues can show up on the logs at different levels. Kaul and Jain's (2019) idea align with the participant experience that the VoIP router logs' levels can range from high to low priority. Participant 3O2 explained the types of information found on VoIP router logs to determine what is happening on the network. Kaur et al. (2017) confirmed timestamps, the destination of IP address, Input and output of numbers, and packet and byte counts on a VoIP router log. On the router, logs are where the network traffic examines an essential source of recorded evidence.

Firmware enhances security features and makes improvements to a VoIP system. Participant 2O3 stood out with their experience with firmware. They stated that it is essential that firmware is continuously updated to ensure that security and bug fixes are up to date. The participant explained that firmware makes security updates that guard against credential theft, preventing hackers from making phone calls on the system. Zheng et al. (2018) acknowledged that firmware helps control a VoIP telephone system's functioning by securing and routing incoming and outgoing phone calls. Participant 1O2 suggested a prompt display when the firmware needs to be updated, alerting you that an update is required. Also, Participant 2O3 indicated that most VoIP phone systems would have an automatic firmware update that the system completes independently. Araneo et al. (2018) confirmed that complying with updating the firmware is an essential part of maintaining a VoIP system. Updating VoIP firmware monthly allows the system to run and automatically reboot to upgrade the VoIP system.

This subtheme, the use of security patches, is supported in the literature because IT security managers need security patches to pinpoint any problems that could go wrong on a VoIP system. For example, Velianitis (2018) stated that security patches are essential to securing a VoIP system to prevent unauthorized access to the network. Tandel and Rughani (2018) wrote that improving VoIP network security is vital to preventing call interception. An IT manager will secure a VoIP network to prevent hackers from tampering and gaining easy access to the network. Suthar and Rughani (2020) stated that IT employees that regularly update patches avoid VoIP attacks and vulnerabilities on the system. The findings to security patches are essential in ensuring a VoIP system is secured and necessary for an IT security manager to control the network and keep it secured.

This subtheme, use of security patches, aligns with the RAT framework because the theory's primary purpose is to prevent a crime from happening. Security patches help to avoid any problems from taking place on a VoIP telephone system. Addesso et al. (2020) confirmed that RAT develops strategies to prevent a crime by monitoring criminal activities. The IT security managers who are the guardians of the VoIP systems in organizations maintain and keep the system from failing using call logs and firmware. Rubio et al. (2019) stated that security controls help minimize VoIP attacks that slow down the system's performance. However, VoIP has security challenges that IT managers must monitor closely to prevent intercepting and misusing data. Ivy and Priya (2018) suggested that monitoring a VoIP system is essential to prevent the system from being compromised. The subtheme, use of security patches, aligns with the theme best practice for VoIP security as IT security managers' concerns are to keep the VoIP system safe from hackers. IT security managers use security patches to protect the system.

Theme 2: Using a Secure VoIP Provider

The second theme that emerged in the participant's interviews was using a secure VoIP provider. Most participants addressed why it is essential to use a secure VoIP provider and reliable providers in this area. Using a secure provider shows how well these precautions protected a VoIP system in telecommunication organizations. The following two subthemes each contain sub subthemes that the participants mentioned.

- VoIP Service Providers
- Network/ Equipment Access

The participant's data ensures that these two subthemes and their sub subthemes are required to secure a VoIP telephone system and keep it from failing. Table 2 shows the data collected from the participants suggest the two subthemes for using a secure VoIP provider when securing a VoIP telephone system.

Table 2

Second Major Theme: Using a Secure VoIP Provider

Subthemes	VoIP Service Providers (d)	Network/ Equipment Access (d)
Participants	9	9

Documents	1	1

Note. d = data collected.

VoIP Service Providers

VoIP service providers are needed to help organizations with the accessibility of connecting to customers from anywhere. Alsoubaie (2019) stated that VoIP service providers are essential in providing services that will keep the organization safe from vulnerabilities. The participants ensured that a service provider is necessary to provide the appropriate Quality of Service needed for the organization's success. When asked what an IT security manager is looking for in a provider, all participants stated they are looking for QoS and low-cost providers. Cortés-Mendoza et al. (2016) noted that a provider's QoS affects call processing and the provider of bills for service costs. The service providers the participants use the most are Verizon, Vonage, and Ring Central.

Telecommunication organizations use Verizon as a Public Switched Telephone Network carrier and Time Division Multiplexing connectivity. Participant 1O2 clarified the organization uses Verizon because the service is reliable and cost-effective. Verizon has excellent Quality when it comes to its reliability. Laghrissi and Taleb (2019) suggested that Verizon has successfully managed large networks even when faced with many challenges with connectivity. In addition, Verizon is cost-effective, allowing the organization to pay for one network for voice calls and data services. Participant 3O2 said that Verizon has a low maintenance fee, and the setup fees were low, making choosing Verizon easy. Shaffer (2017) mentioned that Verizon allows the organization to bundle features such as call forwarding, unlimited calls, voicemails, and email according to the business needs. As a result, the business is saving money on its services. Picking a VoIP service that is helping an organization to save money makes choosing the VoIP provider for their business easy.

Vonage's standard price is cheaper than most VoIP providers. New business customers choose Vonage to receive a VoIP-ready phone and Tech support to support their business. Participant 3O1 informed me that Vonage offers telecommunication company call logs, call readings, call screening, and caller ID. Bukatov et al. (2018) stated that VoIP providers should support VoIP traffic by assessing the issues before they begin. Participant 2O1 said their organization chose Vonage because of their bargaining discounts. Chakraborty et al. (2018) understand why Vonage discounts VoIP services to compete with the other competitors. Participant 1O1 said that the organization uses Vonage to save money on the features. Fatehi and Choi (2018) stated that Vonage is great for business as it protects the company and is less money than the other VoIP telephone providers. Vonage VoIP services are reliable and one of the cheapest VoIP providers available for VoIP services organizations.

Ring Central gives organizations their standard pricing for unlimited calling and premium features. The features for their business customers are the most popular. Participant 2O3 said that Ring Central has many features that the organization uses, including unlimited numbers, 24/7 support, Quality of service reporting, and more. Education Committee (2019) mentioned Ring Central gives the organization a virtual receptionist to help if something goes wrong. Participant 1O3 said that Ring Central recordings could be played back and listened to when needed. Ring Central's call logs record incoming and outgoing phone calls, which helps telecommunication organizations to use their customer's phone numbers for future promotions. Efimov et al. (2017) understand why many organizations are using Ring Central because organizations do not have to worry about updates and upgrades which roll out for free. Participant 3O3 stated that Ring Central is easy to implement as it took half of the day to customize the phone system based on the business needs.

This subtheme, VoIP service providers, is supported in the literature. Service providers improve the communication and collaboration within organizations by securing VoIP transmissions that give high-level security, availability, and support that protects businesses from being compromised. For example, Balamurugan and Biswas (2020) mentioned that having a service provider is essential to alert the organization of any VoIP telephone vulnerabilities. Yihunie and Abdelfattah (2018) stated that service providers must transport secured voice calls over an IP-based VoIP system. The alert will bring attention to IT managers, who can give the VoIP system their full attention to correct the issue. Ravindranath et al. (2017) agreed that choosing a VoIP service provider for any modern business company will benefit the business solutions to manage all incoming calls, audio, and video conferences. The findings to having a service provider that supports a VoIP network are necessary for sending alerts to the IT security manager to know what is going on with the network.

Service providers also align with the theme using a secure VoIP provider and the framework RAT. The RAT theory suggests that when a motivated offender is not going to commit a crime in the presence of a capable guardian. The service provider helps an IT security manager who is the capable guardian guards the VoIP network so that vulnerabilities such as crimes will not occur. Yao-Chung Chang (2019) stated that the motivated offender could act on a crime stopped by the guardian to prevent the crime from happening. An organization that uses a service provider can recognize any mishaps that could take place on their VoIP system and correct it before it becomes a significant concern. Azad et al. (2018) mentioned that collaboration amongst service providers would help catch spammers. Service providers are essential in assisting IT security managers in securing a VoIP telephone system in telecommunication organizations. The subtheme VoIP service providers align with the theme using a secure VoIP provider to assist IT security managers in detecting any vulnerabilities that have taken place on the call logs and either fix or prevent the problem from reoccurring.

Network/ Equipment Access

Network and equipment access is needed to ensure that calls are routed to the correct places, stored, accessed, and monitored. IT Security managers using a secure VoIP provider have access to the network and the equipment needed to run the equipment. Cyrillercel (2020) identified network access as an internet connection for VoIP services. All the participants summarized what a VoIP system needs to work. The answer from all nine participants was for a VoIP system to be at its best. Each phone line should have a minimum network bandwidth connection of 100 kilobytes per second (kbps). Roy and Kumar (2021) agreed with what the participants said to enable VoIP services to operate correctly. In addition, there must be an internet connection of high-speed broadband to convert an analog voice signal into a digital signal. This research proves that using the correct equipment and having the proper network connection can help IT managers to secure a VoIP system in any organization.

VoIP is used over the Internet, making it easy to store data in the cloud. The services cloud provides computing and data storage. Thomas (2020) stated that data storage is a security concern that holds many user-sensitive information. Participant 1O1 advised that VoIP is a cloud-based service used over the Internet on a public IP network that requires an increasing demand for security. Hu et al. (2020) said a cloud VoIP breaks up voice packets into smaller digital packets sent over to the receiver. Participant 1O3 said customers' personal and financial information is sensitive information stored on the cloud. Yang et al. (2019) established that network and data storage are highly used in telecommunication organizations and should be secured to prevent hackers from gaining customer information. Therefore, IT managers need a secure, reliable internet connection for their organization's VoIP system to monitor their customer information stored on a VoIP cloud-based system.

Time-stamped call logs supply records of events that take place over time. Participant 2O3 said that there are error logs. Moffitt et al. (2021) mentioned that VoIP error logs give information about specific errors such as error messages, the time of the error, login, log-out messages, and IP address. IT managers monitor logs to get detailed information and keep track of all the packets entering and leaving the network. Participant 1O2 stated records help find where the problem is in the network so that the IT security manager can troubleshoot the problem. Zahid et al. (2019) confirmed that finding problems within a VoIP system is challenging when the organization's management team does not manage the log. In addition, call volumes do not stay the same in most telecommunication organizations making it hard with multiple calls and visited websites. Participant 1O1 said that storing log information in one place and monitoring the logs with a viewer that detects and alerts with problems can help with the complexity of managing the call logs. Kumar and Roy (2020) confirmed that using VoIP call logs can enhance monitoring and ensure availability and creditability to the organization. Call logs are essential for IT security managers who manage a VoIP telephone system to detect any problems on the system before they begin.

VoIP call audits perform a test to the organization's secure network. Participant 2O2 said that call audits are designed for security issues that result from an unsecured VoIP architecture. Nazih et al. (2020) explained that vulnerabilities found during a VoIP call audit investigate damages made to the organization. The types of injuries that the system can discover are eavesdropping, password cracking, unauthorized changes to the system, and Denial of Services. Participant 1O2 said the purpose of call audits is to provide a clear status of unauthorized penetration and damages to an organization's VoIP network. In addition, McInnes et al. (2019) call logs can help stop hacking attempts in a VoIP network. Many telecommunication organizations use call audits in their call centers to identify gaps, performance improvements, strengths, and weaknesses in an organization.

This subtheme, network and equipment access, is supported in the literature. IT security managers can store, monitor, and route VoIP calls correctly with the information obtained from the audit. For example, Neacsu and Schiopu (2020) stated conducting a

VoIP call audit will ensure that calls are received and sent without errors. When done, audit testing the logs help compare standards configured to a set of parameters.

The network and equipment access subtheme also aligns with RAT because network and equipment allow an IT security manager to manage, detect and store information needed to keep the network system safe from being compromised. Schaefer (2021) suggested RAT detects a crime with the people who play a role in the crime. Those people are the hackers, the IT security managers, and the people in the organization. The network and its equipment help to detect if a crime is going to happen and alert an IT security manager of the dangers or damages on the VoIP system. An IT security managers play an essential role in reading the call logs to correct any changes to the organization is creditable. The subtheme network/equipment access aligns with the theme using a secure VoIP provider to assist IT security managers in doing their jobs of detecting and securing a VoIP system.

Theme 3: VoIP Security Recommendations

The participants recommended ways to secure a VoIP system for their telecommunication organizations, which was the third theme that emerged in the participant's interviews. In this area, most participants addressed keeping the system secured and what practices worked best. Therefore, the VoIP security recommendations are the precautions used and best protect a VoIP system in telecommunication organizations. The following two subthemes each contain sub subthemes that worked best by the participant.

- Implement VoIP Prevention

- Routers with Firewalls for VoIP

The participants' data ensures that these two subthemes are required to secure a VoIP telephone system and keep it from failing. Table 3 shows the two subthemes for VoIP security recommendations to securing a VoIP telephone system.

Table 3

Third Major Theme: VoIP Security Recommendations

Subthemes	Implement VoIP Prevention (d)	Routers with Firewalls for VoIP (d)
Participants	9	9
Documents	1	1

Note. d = data collected.

Implementation of VoIP Prevention

The implementation of VoIP prevention is essential to apply to any VoIP system as an added layer of security to the VoIP server and their applications. Hsieh and Leu (2017) emphasized that implementing VoIP prevention isolates VoIP servers by using the required infrastructures from computers, laptops, and telephones to carry data and voice traffic to its destination correctly. The participants explained that detecting VoIP Activity, prevention measures, and security patches to prevent a VoIP from failing will help secure a VoIP system in telecommunication organizations. Sumi et al. (2019) indicated guidelines to follow when securing a VoIP system such as firewalls, complying with security measures, confidentiality, integrity, availability, and authentication. Participant 3O2 describes what endpoint security provides to an additional layer of protection by blocking malware from infecting the firewall. Also, Participant 2O1 suggested that securely configuring VoIP applications with whitelist country codes is essential to eliminating or reducing toll fraud calls. Lastly, Participant 1O3 added that implementing prevention measures should be one of the first things you do when setting up a VoIP system to proactively monitor any detection of counterattacks. Gandotra and Perigo (2020) agreed with the participants on implementing a VoIP prevention strategy to secure VoIP traffic before it becomes a security concern.

Detecting abnormal activity in a VoIP system obtains real-time traffic reports and checks the reports to notice attack patterns. Kurt et al. (2018) indicated that detecting abnormalities is done by recognizing patterns on the network packets. Participant 3O2 suggested that monitoring the traffic of the organization's VoIP system is vital as it can protect the traffic from a particular IP address. Mousavi and St-Hilaire (2015) emphasized steps to detect which activities are routine and characterize the different attacks on the VoIP network. Participant 2O1 suggested that the attacks are classified. The participants explained that an attacker must go through many stages to achieve the malicious attack, such as figuring out security credentials, information gathering, or passwords. Praseed and Thilagam (2019) agreed that a hacker would send requests in a short period to try to gather information about the users and the servers. Participant 2O3 recommends paying close attention to abnormalities on the VoIP system by treating all the alerts as a severe concern.

Prevention measures for VoIP seem simple with enforcing strong passwords, reviewing call logs, restricting calls, deactivating inactive accounts, and choosing a secure VoIP provider. Participant 3O2 suggested looking for strange behavior on the VoIP network; usually, it is the first sign that something could go wrong. Bahnasse et al. (2018) indicated looking for packets that are not in the correct order and within a reasonable time to reproduce the voice appropriately. Participant 2O1 suggested that good detection performance is required when maintaining your VoIP network, such as looking for parameters and factors that show a variation of call patterns on the VoIP system. Holub et al. (2018) agreed that the longer the call duration, the better the call, motivating the relation between call quality and duration. Participant 3O1 monitors the impairments in calls to see which calls have differences between the beginning and termination times. Yihunie and Abdelfattah (2018) agreed that telecommunication organizations detect attack patterns and solve the problems before an issue with the network. Detecting anomalies in VoIP networks before they are serious is the focus of all the participants who work in telecommunication organizations.

This subtheme, implementation of VoIP prevention, is supported in the literature. Prachi (2021) agreed that seeing amoralities before they become a problem is beneficial to any organization that supports a VoIP network. Detection of a VoIP system will help the IT security manager secure the internal system so hackers cannot intercept data within the organization. Baykara and Das (2018) noted that IT security managers could use a checklist to help with identifying all precautions taken when securing the network, starting with detecting firewalls that can detect traffic to a VoIP network. Troubleshooting VoIP issues on the network could help save time and loss of performance in the organization. Roy et al. (2018) indicated detecting problems on a

VoIP network before they become a significant problem can resolve call quality issues the first time they occur. Detecting any flaws on the VoIP network is vital to an IT security manager. Having a prevention method helps pinpoint the problem before it becomes an issue.

This subtheme, implementation of VoIP prevention, aligns with RAT. It shows that finding the VoIP problems before it becomes a more significant situation is pivotal to keeping the VoIP network under control in telecommunication organizations. Javed et al. (2021) asserted that it is crucial to focus on all malicious attacks on the network. Targeting the signaling flow that characterizes the attacks between what is abnormal helps pinpoint where the attacks are coming from in the VoIP environment. Safoine et al. (2018) suggested that using the feedback from the signaling flow on VoIP detections will extend the ability to fix and detect ongoing attacks. The RAT framework avoids situations before they become a problem why RAT frameworks resonate with this research study. The subtheme implementation of VoIP prevention aligns with the theme VoIP security recommendations

Routers with Firewalls for VoIP

In telecommunication organizations**,** routers with firewalls for VoIP are essential to connecting incoming and outgoing phone calls over the Internet. Participant 3O3 said that the router aims to combine multiple networks or forward packets to their destination. Radcliffe et al. (2019) suggested that VoIP routers can impact your call quality and connectivity. Participant 1O1 emphasized that data packets are sent through VoIP traffic and can be mismanaged or lost. Daoud and Qu (2019) agreed that phone calls would not go through if a router does not receive VoIP data packets. Participant 3O2 believes that a router is the heart of a VoIP network. Mahjabin et al. (2017) agreed that VoIP routers are the first defense against attacks because most routers have a built-in firewall protecting the network. All the participants agreed that having a router with firewalls is vital for maintaining a VoIP system.

Telecommunication organizations use a router with 802.11n to implement wireless local area network speed. Perwej (2017) suggested all routers that broadcast in 802.11n are ideal for most traffic in VoIP. 802.11n uses 5GHZ and 2.4 GHz for faster voice travel from the sender to the receiver. Participant 2O2 stated 802.11n are wireless networks commonly used in organizations because they are suitable for VoIP and cloud applications. Estepa et al. (2018) agreed that 802.11n improves the energy efficiency of a VoIP system, so maintaining the system ensures speech quality and Quality of service. Participant 3O1uses the 802.11n technology to transmit multiple data through multiple-input and multiple-output processes signals for various data streams. Dhar and Chatterjee (2017) suggested that 802.11n reduces noise and interference by reducing the access delay to the network. Therefore, 802.11n is essential for keeping a VoIP system safe and the voice traffic moving smoothly.

Ubiquiti and Cisco Adaptive Security Appliance (ASA) is a router that allows control of the network's system traffic by the participants in this study. Ubiquiti combines a router, four ethernet ports, and a Wi-Fi access point. Cisco ASA router combines firewall, antivirus, and Intrusion for security prevention. Cisco ASA provides a defense that stops attacks before spreading throughout the network. Ubiquiti offers excellent value and an easy installation. Participant 2O1 said that Ubiquiti is cost-effective hardware. Cobo-Simón and Tamames (2017) agreed that Ubiquiti has a lower cost than its competitors. Participant 1O3 said that Ubiquity does not charge software licensing or maintenance fees. Talla et al. (2017) agreed that Ubiquity is fantastic hardware used both short and long term. Cisco ASA helps organizations increase their capacity and improve their performance by delivering high application availability. Participant 2O2 said Cisco provides context awareness with Cisco's security group tags and identity-based technology. Ramachandran (2019) agreed that Cisco is user-friendly and compatible with equipment.

This subtheme, routers with firewalls for VoIP, is supported in the literature. Neupane et al. (2018) noted that having a firewall is essential for a network security strategy. An IT security manager's primary focus is to eliminate the chances of being hacked, and building a firewall is the first line of defense against an attack. Steinmetzer et al. (2018) supported the participant's experiences by stating that the router security requirement addresses privacy from man-in-middle attacks, eavesdropping, and interruption of data packets. Attaran et al. (2019) expressed that if a router is new, the organization increases the levels of undesirable activity. IT security managers know which router and firewall work well with the organization because it is essential in securing a telecommunication organization VoIP system.

Related to the RAT conceptual framework, this subtheme routers with firewalls for VoIP suggests that VoIP security recommendations tie into the whole process of an IT security manager using routers and firewalls to secure a telecommunication organization's VoIP system, which supports the findings of Skerpac (2019). Cohen and Felson (1979) opined that RAT supports the opportunity to control a crime from taking place by decreasing the crime that may bring forth a criminal activity. Using a firewall will enhance security, and the chances of criminal activity on a VoIP system in telecommunication organizations will be minimal. Furthermore, an IT security manager will improve the performance of the organization's VoIP system when using a router that supports the organization's needs. These findings are tied to RAT with firewalls and routers to sustain VoIP security in telecommunication organizations, minimizing hackers from compromising the VoIP system. The subtheme routers with firewalls for VoIP aligns with the theme VoIP security recommendations because it is essential to secure a VoIP network.

Theme 4: Awareness of Future Security Concerns

Many participants had future security concerns about what could happen if some of these precautions were mishandled. The participants had doubts about what could happen in the future if a telecommunication organization's VoIP system is not secured and how they can do something about it before destruction happens, which was the fourth theme that emerged in the participant's interviews. In this area, most participants address security measures used today to eliminate any future breaches. The following two subthemes each contain sub subthemes that were considered best by the participants.

- Customer Proprietary Network Information (CPNI)
- For additional consideration

The participants' data ensures that these subthemes are required to secure a VoIP telephone system and keep it from failing. Table 3 shows the participants' data suggest the subthemes for VoIP security recommendations to securing a VoIP telephone system.

Table 4

Fourth Major Theme: Awareness of Future Security Concerns

Subthemes	Customer Proprietary Network Information (CPNI) (d)	For Additional Consideration(d)
Participants	9	9
Documents	1	1

Note. d = data collected.

Customer Proprietary Network Information

Customer Proprietary Network Information (CPNI) is enforced through The U.S. Telecommunication Act of 1996, guaranteeing the Federal Communication Commission (FCC) that all consumers' information is private. The data collected by telecommunication organizations about their customer's telephone calls and confidential information should remain secure. The one document that I obtained from participant 1, organization 3, was a signed CPNI document that ensured that the organization followed the FCC rules that govern CPNI. The document outlines the organization's procedures for accessing, using, and storing customers' Proprietary Network Information. Bougiakiotis (2020) acknowledged that CPNI prohibits using customers' information to be purchased. Under federal law, CPNI also includes all available information on a telephone bill which consists of a customer's phone number, call information, and calling patterns. Participant 1O3 signed the document ensuring compliances with the FCC’s rules that govern the

CPNI laws. Guidry (2019) expressed that CPNI is not used for activities involving other parties, only those required to disclose to federal law. The CPNI law prohibits releasing a customer's password, address, and telephone number.

The U.S. Federal Trade Commission (FTC) protects customers' privacy from telecommunication services. Huang et al. (2017) said the FTC protects people's rights by stopping deceptive and fraudulent practices. Participant 2O2 believes the FTC contains unfair acts by investigating organizations that may break the law. The participant is glad that the FTC never audited the organization. Manne et al. (2018) stated that the rules that the FTC put in place help educate consumers and help stop the violations of laws. The FTC issued orders to telecommunication organizations, such as Verizon, Comcast, and AT&T, to use customer data (Boyne, 2019). Participant 2O3 said the FTC wants to know what types of data organizations gather. Peha (2016) noted that the FTC seeks to understand how much personal data is shared with third parties giving access to customer information. The FTC allows customers to access this information and delete their information from being viewed.

The Communication Act of 1934 is a federal law that provides a foundation for telecommunications policies for telephone communication. Meghani (2017) wrote the Federal Communications Commission regulates and oversees technology in customer homes. Participant 1O3 said that the FCC updated the communication act in 1996 to define competition of the communication market, which tells telecommunications organizations what is done legally to keep their services safe. Delp and Mayo (2016) stated that the FCC is responsible for interstate and foreign communications regulations for radio, television, satellite, and wires.

The Payment Card Industry Data Security Standard (PCI-DSS) ensures that the processing of credit card information is secured. PCI-DSS mandates that Virtual Local Area Networks (VLAN) must be secured. PCI- DSS compliance is a certificate that groups get to meet all PCI-DSS requirements. Rahaman et al. (2019) expressed that securing your customers' payment is vital for every organization. If an organization does not comply with the PCI-DSS rules, the organization will risk penalties to the organization. Elluri et al. (2018) supported what Participant 3O2 said about organizations with e-commerce websites needing to prove to the bank they are qualified to handle and process information securely. All organizations must obtain a PCI-DSS security certification to do business with a bank over the Internet. Participant 2O1 stated that many telecommunication organizations use PCI-DSS to store their customer's data. Elluri et al. (2018) stated that for an organization to be PCI-DSS approved, the organization must record and store all conversations about the customers' credit card information. PCI-DSS is an agency that makes sure the organization collecting credit card information is safe and has all the capabilities of being a secured organization before allowing the organization access to customers' information.

This subtheme, the use of the Customer Proprietary Network Information, is tied to the literature review because an organizational document secures details about the customer's telecommunication services. Saxena et al. (2020) mentioned that CPNI has customers' sensitive information, call logs, and purchased services. Participant 1O3 said that the primary purpose of CPNI is to create directories that organizations cannot use for soliciting. Frieden (2019) discussed the primary purpose of CPNI is to give telephone details such as charges, local and long-distance calls, and other types of services on a bill. The customer's information is kept unpublished and unknown to the public through the agreements of CPNI. Rither and Hoxie (2017) agreed that CPNI is important in telecommunication organizations because CPNI legally secures customers' profile and telephone account information. IT security managers keep the customers safe and the organizations by making sure that the CPNI is always up to date and the organization is staying within the guidelines of the FCC.

Use of CPNI is aligned with RAT because CPNI secures the organization and its customer's information. IT security managers secure the organization by securing the VoIP telephone system when they are charging customers' credit cards and information. The RAT theory emphasizes keeping a crime secured before it happens, just like an IT security manager needs to keep the organization from hackers. Eck and Madensen (2018) mentioned that if a guardian is absent, then the likelihood of a crime happening is one hundred percent, but there will be no crime if there are people around. The same goes for IT security managers, CPNI, FCC, and PCI-DSS. If IT security managers are present, the likelihood of a crime is at zero percent, but without these factors, an organization does not have protection from people who commit crimes. These findings are tied to RAT so IT security managers can be aware of what can happen if an IT security manager is not following the rules of CPNI, FCC, and PCI-DSS rules.

Future Consideration

The future security concerns were an additional consideration of future security measures for VoIP. Participant 3O2 stated that customers educated on securing their information when using their VoIP telephone system supported by any telecommunication organization would know how to secure their data. Participant 1O3 indicated that customers are unaware that people could eavesdrop on their conversations. Roy and Kumar (2021) reported that VoIP services are becoming used more within organizations, increasing security concerns, such as more ways for hackers to invade the VoIP system. A security regulation will help customers and IT security managers feel confident that their VoIP system is secured.

Proper education on securing a VoIP telephone service would help IT security managers learn from other IT security managers how to keep their VoIP system secured if sufficient education is provided to the customers of those organizations that use a VoIP system. Participant 2O3 said that the organization provides each new customer information about their new phone system and security while using their telephone system. Furnell (2020) stated that many organizations tell customers about cybercriminals and ways to protect their passwords from being compromised. Participant 3O3 noted that cybercriminals get into your ports through DDoS attacks, which send many requests to attack the web source in hopes the web source stops functioning. It then floods the system, making the VoIP service drop skip calls. Payne and Abegaz (2017) mentioned protecting your VoIP service with malware, regularly changing your password, and limiting the device used for the internet. Customers who follow securing their VoIP services should be safe when putting their private information over the internet.

Organizations that protect their VoIP system should enforce strong password policies that include changing the password every 3 months. Participant 2O2 insists that alerting call logs helps alert the IT security managers if something is wrong with the VoIP system. Kaur et al. (2017) expressed call logs give detailed information of outgoing and incoming calls specifying the call history. Participant 1O3 said that applying operating system updates often helps with security fixes that can enhance features and improve the stability of the software. Naeem et al. (2020) confirmed that protecting the VoIP network from threats helps with vulnerabilities on the network. All updates on the VoIP network aim to remove outdated features and add new features that can improve the software.

Lastly, for future consideration for organizations that think about having more than one way to secure their VoIP system, all the participants suggest using an all cloud-based VoIP system or a hybrid VoIP system. Wagdy et al. (2021) proposed a cloud-based VoIP system in one area and a Private Branch eXchange (PBX) in another region. Participant 3O1 recommended that the PBX be used for people working in the office. The cloud-based VoIP system would be for any employees working remotely from anywhere, which will benefit the organization because it will be fault-tolerant. The likelihood of the organization losing VoIP phone services because of a disaster is minimal. Dinar et al. (2020) suggested hybrid VoIP is the best of both worlds when you combine IP and analog services to an organization. Participant 2O3 said that an organization that uses a hybrid VoIP system provides flexibility because it allows it to grow to other areas. For example, suppose the organization is in New York. In that case, the organization can employ employees from across the globe to work from home, allowing the organization to branch out to other areas.

This subtheme, future considerations for VoIP, is supported in the literature because the future of VoIP technology is an internet protocol that will be around for years. Abualhaj et al. (2019) stated VoIP security is the future of business and needs an improved security protocol. Participant 2O1 said that VoIP is more secure than a few years ago, making VoIP better than the old phone system. Salahdine and Kaabouch (2019) insisted that having a trusted VoIP provider will help with ensuring any suspicious behaviors will be detected and fixed. Participant 1O3 said that VoIP will always need consistent updates to secure its customers. Therefore, the future of VoIP is essential for this literature view as IT security managers work hard at making sure that the future of VoIP is secured and helping the organization improve security with their customers.

Future consideration and CPNI of VoIP are aligned with RAT. Clarke (2018) suggested RAT is a crime prevention methodology focusing on the elements that make up a crime. The future of VoIP concentrates on finding ways to keep a VoIP system from failing. DeLiema (2017) stated to prevent a crime most effectively. The focus must be on all three elements that make up RAT: the target, the capable guardian, and the offender. To effectively secure a VoIP telephone system requires an IT security manager to stop an attacker from gaining access to an organization and its customer's private information. These findings are tied to RAT because the future of VoIP telephone services is essential to all organizations, and knowing what strategies work best to keep a VoIP service secured is necessary.

Application to Professional Practice

The purpose of this qualitative multiple case study explored the strategies used by IT security managers in telecommunication organizations to secure a VoIP telephone system in New York. This research study's findings may contribute to business practices and help IT security managers effectively manage and secure a VoIP telephone system. Analyzing its conceptual framework, RAT and the academic literature helped with VoIP security strategies to increase the knowledge of intercepting and misusing. The findings are related to IT security managers who secure a VoIP telephone system in telecommunication organizations to enhance the organization's telephone system's operational safety. The participant of this study contributes to helping secure a VoIP system within their organizations.

VoIP services are used every day, and technology is growing every day. Keeping VoIP services secured is required by ensuring that a system is in place to monitor VoIP services to help avoid security breaches. IT security managers who provide successful security strategies to keep their organization's VoIP system secured can help other organizations be successful and allow customers to feel safe when using their VoIP services in their homes or business. Salahdine and Kaabouch (2019) believed that when hackers have intercepted an organization's VoIP system, it loses the customer's trust in the organization. In this study, all IT security managers suggest proper training, and customers are supplied with a welcome package to secure their information.

All the strategies used by the IT security managers will secure a VoIP system, improve the organization's VoIP system, and help customers to keep their system secured in their homes and business. In addition, the security strategies used, such as authentication, authorization, confidentiality, and encryption, can be best practices for IT security managers.

Implications for Social Change

The implication for social change from the findings of this study may be helpful to an organization's reputation to help decrease identity theft, credit card theft, and help their customers feel secure when using their services. The findings from this study can add knowledge to IT security managers in telecommunication organizations. The findings can help to prevent VoIP telephone data from being intercepted and misused. This study will result in a positive social change. IT security managers know about implementing security strategies to a VoIP system, so the more secure customers will be.

The findings explain when IT security managers use their security strategies to secure a VoIP system, it improves the organization and the customer satisfaction for feeling secure. The study's findings identified the necessary reasons for securing a VoIP system, protecting organizations and customers from credit cards, and identifying theft. The study findings identify essential for securing a VoIP system in telecommunication organizations, which will protect the organization and its customers from intercepting their telephone service. The study findings have provided an in-depth analysis of the security strategies used by IT security managers, which will positively impact social change by protecting the organization and their customer's information. The security strategies used by IT managers will protect the organization and make the customer feel secure, making the customers that use VoIP services from telecommunication organizations have confidence in the service they are using. Customers need education when signing up for VoIP services with a welcome package that will inform the customers about sharing personal information over the telephone. The security strategies used by IT security managers will protect the organization's VoIP system and help secure the organization from data breaches and call interception.

Recommendations for Action

The finding from this study divulged the key security strategies that IT security managers use to secure a VoIP system. The security strategies to prevent interception and data breaches are essential and must be addressed by IT security managers because VoIP technology is forever evolving. Therefore, implementing a security protocol should be in place for any VoIP telephone system. The strategies that have been effective from this study for IT security managers include:

- Use best practices for VoIP security
- Use a secure VoIP provider
- Follow VoIP security recommendations
- Be aware of future security concerns

I recommend that each organization have a monitoring system to detect breaches before they become severe. Detecting abnormities on a VoIP network is crucial to ensuring that the organization and its customer's information are secured. Next, I recommend that organizations create a training program for their new and old customers on securing their information. It is essential to train or inform customers who use a VoIP telephone system to help them utilize the services to their fullest potential without increasing security problems. Also, I recommend that organizations reinforce the importance of VoIP security. The benefits of strengthening VoIP security will promote a reliable organization that customers are satisfied to refer new customers. Finally, I recommend that organizations have a secondary way of getting customers' information in place. Usually, customer verbally gives their information over the phone. Organizations should develop a way to block out numbers when paying with a credit card. These findings support the current literature on security strategies used to secure a VoIP telephone system. The conclusions of this study are essential to the organization that uses a VoIP telephone system in their organizations.

The participants in this study are adamant about the importance of securing a VoIP telephone system. In addition, the IT security managers suggested that with VoIP becoming popular with telecommunication organizations, security challenges will need the IT security manager's attention.

I will disseminate the results from this study after receiving CAO approval. I will send the research results to all nine of the participants. Also, I will share this study in ProQuest, where other scholars can view and use my research. Finally, I will present this study's findings at security conferences, seminars, and as many people who will listen.

Recommendations for Further Study

The findings of this study shared security strategies used by IT security managers to secure a VoIP telephone system in telecommunication organizations. However, if the limitation of the study was done in New York, repeating this study in a different geographical region of the United States based on the security requirements using a different conceptual framework and methodology will assist organizations and IT security managers in securing a VoIP telephone system.

This study added the security strategies used by IT security managers to secure a VoIP telephone system. However, additional research is needed due to the small sample size of the qualified IT security managers and the telecommunication organizations used in the study. Therefore, future work may explore the security strategies with three telecommunication organizations and larger sample size. Nevertheless, the study has contributed to the literature on security strategies for securing VoIP telephone systems in telecommunication organizations. Therefore, it may be beneficial not just for telecommunication organizations but to all organizations that use a VoIP system.

Lastly, some critical issues that should be addressed in securing a VoIP system in telecommunication organizations in a recommendation for future research topics were:

- Researchers should explore an encryption approach to receiving credit card information from customers over the Internet.
- Researchers should explore an approach that will invest in a security strategy to quickly determine if the network is compromised without running a test.
- Researchers should explore one security strategy to minimize attackers from compromising the system and protect a VoIP telephone system.

Reflections

This research process has been a long journey, but I developed as a person and a doctoral scholar. My understanding of the topic has grown so much over this journey. I was challenged and exhausted at times, but the energy and detail in planning were exciting. I was overwhelmed during the prospectus, proposal, and final phases, but it was all worth it. I was interested in how telecommunication organizations secure their VoIP telephone system after watching someone write their customer's information on a piece of paper. I was curious if someone is listening to the phone conversation between the rep and the client. What if someone is eavesdropping on their telephone conversation? As a data analyst walking through a call center that used a VoIP telephone system, I wondered how the organization is securing its VoIP telephone system. I was motivated to know and decided to write this study.

As an IT professional with over 20 years of experience, I had bias before conducting this study about IT security managers' strategies. I thought about many different strategies used. I minimized my bias when the participants expressed themselves when asking open-ended interview questions, and I listened without giving my opinion. As a result, the participant's results from the semi structured interviews were authentic and from the participant's experiences.

Summary and Study Conclusions

Securing a VoIP telephone system in telecommunication organizations is essential to organizations that use VoIP telephones to keep their system safe from attackers obtaining their customers' personal information who use their services. The purpose of this qualitative multiple case study was to explore the strategies used to secure a VoIP telephone system used by IT security managers in telecommunication organizations for improving data from being intercepted and misused. The specific IT problem was that some IT security managers in telecommunication organizations lack strategies to secure a VoIP telephone system from intercepted and misused data. This qualitative multiple case study investigated security strategies used by IT security managers for securing a VoIP telephone system. The study answered the research question: What strategies do IT security managers use in telecommunication organizations to secure a VoIP telephone system from intercepted and misused data? Nine out of 12 IT security managers from three telecommunication organizations in New York State participated in semi structured interviews. This study indicated that the following are security strategies used by IT security managers to secure a VoIP telephone system:

- Use best practices for VoIP security
- Use a secure VoIP provider
- Follow VoIP security recommendations
- Be aware of future security concerns

There will always be a need for security for VoIP because VoIP is used over the internet, and there will be attackers trying to intercept data and misuse personal information for their gain. Therefore, security problems with VoIP will always be an issue that organizations would have to address. These organizations would need to implement security strategies to keep control over the VoIP system to prevent the organization from being compromised (Seaman, 2021). If all security issues are addressed and resolved with VoIP, this would minimize identity and credit card theft and help customers feel confident and trust using organizations for their VoIP telephone needs.

References

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: Preserving security and privacy. *Journal of Big Data*, *5*(1). http://doi.org/10.1186/s40537-017-0110-7

Abro, M. M. Q., Khurshid, M. A., & Aamir, A. (2015). The use of mixed methods in management research. *Journal of Applied Finance and Banking, 5*(2), 103-108. https://www.journals.elsevier.com

Abualhaj, M. M., Al-Tahrawi, M. M., & Al-Khatib, S. N. (2019). A new method to improve voice over IP (VoIP) bandwidth utilization over internet telephony transport protocol (ITTP). *Proceedings of the 2019 8th International Conference on Software and Information Engineering*. https://doi.org/10.1145/3328833.3328885

Adah Agana, M., & Wario, R. (2018). A multi-level evidence-based cyber crime prosecution information system. *International Journal of Engineering & Technology, 7*(3.19), 39. https://doi.org/10.14419/ijet.v7i3.19.16985

Addesso, P., Cirillo, M., Di Mauro, M., & Matta, V. (2020). VoIP: Adversarial detection of encrypted and concealed VoIP. *IEEE Transactions on Information Forensics and Security, 15*, 943-958. https://doi.org/10.1109/tifs.2019.2922398

Adu, P. (2019). Using Dedoose to analyze qualitative data. *A Step-by-Step Guide to Qualitative Data Coding*, 278-328. https://doi.org/10.4324/9781351044516-12

Airi, P., & Anderson, P. K. (2017). Cisco Packet Tracer as a teaching and learning tool for computer networks in DWU. *Contemporary PNG Studies*, *26*, 88-108. https://www.researchgate.net/publication/329453806

Akinbami, J., Virtanen, S., & Sainio, P. (2018). *Developing best practices for securing VoIP communication for a non-profit organization.* https://www.utupub.fi/handle/10024/146559

Alaba, F. A., Othman, M., Hashem, I. A., & Alotaibi, F. (2017). Internet of things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28. https://doi.org/10.1016/j.jnca.2017.04.002

Alajmi, N. K., Haj Aliwi, H. S., & Alieyan, K. (2017). VoIP protocols' bandwidth based-mini/RTP header using different codecs: A comparison. *Asian Journal of Scientific Research*, *10*(3), 110-115. https://doi.org/10.3923/ajsr.2017.110.115

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), 9-19. https://doi.org/10.7575/aiac.ijels.v.5n.2p.9

Algozzine, B., & Hancock, D. (2016). *Doing case study research: A practical guide for beginning researchers* (3rd ed.). https://eric.ed.gov/?id=ED572667

Ali, Z., Naz, F., Qurban, M., Yasir, M., & Jehangir, S. (2020). Analysis of VoIP over wired & wireless network with implementation of QoS CBWFQ & 802.11e. *International Journal of Computer Network and Information Security, 12*(1), 43-49. https://doi.org/10.5815/ijcnis.2020.01.005

All, A., Nuñez Castellar, E. P., & Van Looy, J. (2016). Assessing the effectiveness of digital game-based learning: Best practices. *Computers & Education*, *92-93*, 90-103. https://doi.org/10.1016/j.compedu.2015.10.007

Allen, R. E., & Wiles, J. L. (2016). A rose by any other name: Participants choosing research pseudonyms. *Qualitative Research in Psychology*, *13*(2), 149-165. https://doi.org/10.1080/14780887.2015.1133746

Alouneh, S., Abed, S., & Ghinea, G. (2016). Security of VoIP traffic over low or limited bandwidth networks. *Security and Communication Networks*, *9*(18), 5591-5599. https://doi.org/10.1002/sec.1719

Alsoubaie, F. (2019). Using the hierarchical decision model (HDM) to select a sustainable Voice over Internet Protocol (VOIP) provider. In *2019 Portland International Conference on Management of Engineering and Technology* (pp. 1-9). IEEE. https://doi.org/10.23919/PICMET.2019.8893927

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*(3). https://www.ncbi.nlm.nih.gov/pubmed/29694754

Araneo, A., Gamess, E., & Urribarri, D. (2018). A set of policies and guidelines for deploying safer VoIP solutions. *International Journal of Computer Theory and Engineering*, *10*(2), 46-53. https://doi.org/10.7763/ijcte.2018.v10.1197

Argun, U., & Dağlar, M. (2016). Examination of routine activities theory by the property crime. *International Journal of Human Sciences*, *13*(1), 1188. https://doi.org/10.14687/ijhs.v13i1.3665

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.org/10.1093/jcr/ucx096

Ashby, M. P., & Tompson, L. (2017). Routine activities and proactive police activity: A macro-scale analysis of police searches in London and New York City. *Justice Quarterly*, *34*(1), 109-135. https://doi.org/10.1080/07418825.2015.1103380

Attaran, M., Attaran, S., & Kirkland, D. (2019). The need for digital workplace. *International Journal of Enterprise Information Systems*, *15*(1), 1-23. https://doi.org/10.4018/ijeis.2019010101

Azad, M. A., Morla, R., & Salah, K. (2018). Systems and methods for SPIT detection in VoIP: Survey and future directions. *Computers & Security*, *77*, 1-20. https://doi.org/10.1016/j.cose.2018.03.005

Bahnasse, A., Badri, A., Louhab, F. E., Talea, M., Khat, A., & Pandey, B. (2018). Behavior analysis of VoIP performances in next-generation networks. *International Journal of Engineering & Technology*, *7*(3.15), 353-359. https://www.sciencepubco.com/index.php/ijet/article/view/21383

Balamurugan, B., & Biswas, D. (2020). Security in network layer of IoT. *Securing the Internet of Things*, 190-212. https://doi.org/10.4018/978-1-5225-9866-4.ch011

Banerjee, M., Lee, J., & Choo, K. R. (2018). A blockchain future for internet of things security: A position paper. *Digital Communications and Networks*, *4*(3), 149-160. https://doi.org/10.1016/j.dcan.2017.10.006

Basem, B., Ghalwash, A. Z., & Sadek, R. A. (2015). Multilayer secured SIP-based VoIP architecture. *International Journal of Computer Theory and Engineering, 7*(6), 453-462. https://doi.org/10.7763/ijcte. 2015.V7.1002

Baykara, M., & Das, R. (2018). A novel honeypot based security approach for real-time intrusion detection and prevention systems. *Journal of Information Security and Applications*, *41*, 103-116. https://doi.org/10.1016/j.jisa.2018.06.004

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

Bensalah, F., Kamoun, N. E., & Bahnasse, A. (2017). Scalability evaluation of VOIP over various MPLS tunneling under OPNET Modeler. *Indian Journal of Science and Technology*, *10*(29), 1-7. https://doi.org/10.17485/ijst/2017/v10i29/117369

Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. *Qualitative Research*, *15*(2), 219-234. https://doi.org/10.1177/1468794112468475

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2016). E-LDAT: A lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric. *Security and Communication Networks*, *9*(16), 3251-3270. https://doi.org/10.1002/sec.1530

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*(13), 1802-1811. https://doi.org/10.1177/1049732316654870

Bogers, M., Zobel, A. K., Afuah, A., Almirall, E., Brunswicker, S., Dahlander, L., Frederiksen, L., Gawer, A., Gruber, M., Haefliger, S., Hagedoorn, J., Hilgers, D., Laursen, K., Magnusson, M. G., Majchrzak, A., McCarthy, I. P., Moeslein, K. M., Nambisan, S., Piller, F. T., … Ter Wal, A. L. J. (2017). The open innovation research landscape: Established perspectives and emerging themes across different levels of analysis. *Industry and Innovation, 24*(1), 8-40. https://doi.org/10.1080/13662716.2016.1240068

Bogoslavskyi, I., & Stachniss, C. (2017). Analyzing the quality of matched 3D point clouds of objects. *2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. https://doi.org/10.1109/iros.2017.8206584

Bougiakiotis, E. (2020). The layered links model: An alternative approach to international privacy regulation. *International Data Privacy Law*, *10*(3), 253-268. https://doi.org/10.1093/idpl/ipaa002

Boyne, S. M. (2019). Data protection in the United States: U.S. national report. *Ius Comparatum - Global Studies in Comparative Law*, 409-455. https://doi.org/10.1007/978-3-030-28049-9_17

Bravo, S., & Mauricio, D. (2018). DDoS attack detection mechanism in the application layer using user features. *2018 International Conference on Information and Computer Technologies (ICICT)*. https://doi.org/10.1109/infoct.2018.8356848

Bree, R. T., & Gallagher, G. (2016). Using Microsoft excel to code and thematically analyze qualitative data: a simple, cost-effective approach. *AISHE-J: The All Ireland Journal of Teaching and Learning in Higher Education*, *8*(2). http://ojs.aishe.org

Brehmer, M., Lee, B., Bach, B., Riche, N. H., & Munzner, T. (2017). Timelines revisited: A design space and considerations for expressive storytelling. *IEEE Transactions on Visualization and Computer Graphics*, *23*(9), 2151-2164. https://doi.org/10.1109/tvcg.2016.2614803

Brennan, T. (2016). The post-internet order broadband sector: Lessons from the pre-open internet order experience. *Review of Industrial Organization*, *50*(4), 469-486. https://doi.org/10.1007/s11151-016-9551-y

Bromley, E., Mikesell, L., Jones, F., & Khodyakov, D. (2015). From subject to participant: Ethics and the evolving role of community in health research. *American Journal of Public Health*, *105*(5), 900-908. https://doi.org/10.2105/ajph.2014.302403

Brown, G., Strickland-Munro, J., Kobryn, H., & Moore, S. A. (2017). Mixed methods participatory GIS: An evaluation of the validity of qualitative and quantitative mapping methods. *Applied Geography*, *79*, 153-166. https://doi.org/10.1016/j.apgeog.2016.12.015

Bryan, C., Ma, K., & Woodring, J. (2017). Temporal summary images: An approach to narrative visualization via interactive annotation generation and placement. *IEEE*

Transactions on Visualization and Computer Graphics, *23*(1), 511-520. https://doi.org/10.1109/tvcg.2016.2598876

Bukatov, A. A., Polukarov, D. Y., Zaitsev, N. D., & Sukhov, A. M. (2018). On improving the Quality of VoIP connections. *Data Science*. https://doi.org/10.18287/1613-0073-2018-2212-366-371

Busse, C., Kach, A. P., & Wagner, S. M. (2017). Boundary conditions. What they are, How to explore them, Why we need them, and When to consider them. *Organizational Research Methods*, *20*(4), 574-609. https://doi.org/10.1177/1094428116641191

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

Cha, B., Kim, J., Moon, H., & Pan, S. (2017). Global experimental verification of docker-based secured mVoIP to protect against eavesdropping and DoS attacks. *EURASIP Journal on Wireless Communications and Networking*, *2017*(1), 63. https://doi.org/10.1186/s13638-017-0843-1

Chahid, Y., Benabdellah, M., & Azizi, A. (2017). Internet of things security. *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*. https://doi.org/10.1109/wits.2017.7934655

Chakraborty, T., Misra, I. S., & Prasad, R. (2018). Overview of VoIP technology. *Springer Series in Wireless Technology*, 1-24. https://doi.org/10.1007/978-3-319-95594-0_1

Chang, J. S., Jeon, Y. H., Sim, S., & Kang, A. N. (2015). Information security modeling for the operation of a novel highly trusted network in a virtualization environment. *International Journal of Distributed Sensor Networks*, *11*(9), 359170. https://doi.org/10.1155/2015/359170

Chaudhry, S. A., Naqvi, H., Sher, M., Farash, M. S., & Hassan, M. U. (2017). An improved and provably secure privacy-preserving authentication protocol for SIP. *Peer-to-Peer Networking and Applications, 10*(1), 1-15. https://doi.org/10.1007/s12083-015-0400-9

Chen, W., Guan, Q., Jiang, S., Guan, Q., & Huang, T. (2016). Joint QoS provisioning and congestion control for multi-hop wireless networks. *EURASIP Journal on Wireless Communications and Networking*, *2016*(1). https://doi.org/10.1186/s13638-016-0519-2

Choi, K., Choo, K., & Sung, Y. (2016). Demographic variables and risk factors in computer-crime: An empirical assessment. *Cluster Computing*, *19*(1), 369-377. https://doi.org/10.1007/s10586-015-0519-8

Choi, K., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394-402. https://doi.org/10.1016/j.chb.2017.03.061

Clarke, R. V. (1980). “Situational” crime prevention: Theory and practice. *The British Journal of Criminology*, *20*(2), 136-147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

Clarke, R. V. (2018). The theory and practice of situational crime prevention. *Oxford Research Encyclopedia of Criminology and Criminal Justice*. https://doi.org/10.1093/acrefore/9780190264079.013.327

Clarke, R. V. (2018a). The links between realistic evaluation and situational crime prevention. *Realist Evaluation for Crime Science (pp. 47-57).* Routledge. https://doi.org/10.4324/9781315627144

Clough, J. (2015). Towards a common identity? The harmonization of identity theft laws. *Journal of Financial Crime, 22*(4), 492-512. https://doi.org/10.1108/jfc-11-2014-0056

Coates, J. F. (2016). The future of federal city- Washington, DC. *Technological Forecasting and Social Change*, *113*, 47-50. https://doi.org/10.1016/j.techfore.2016.10.047

Cobo-Simón, M., & Tamames, J. (2017). Relating genomic characteristics to environmental preferences and Ubiquity in different microbial taxa. *BMC Genomics*, *18*(1). https://doi.org/10.1186/s12864-017-3888-y

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. https://doi.org/10.2307/2094589

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review*, 46, 505-524. https://doi.org/10.2307/2094935

Colp, P., Zhang, J., Gleeson, J., Suneja, S., De Lara, E., Raj, H., & Wolman, A. (2015). Protecting data on smartphones and tablets from memory attacks. *ACM SIGARCH Computer Architecture News*, *43*(1), 177-189. https://doi.org/10.1145/2786763.2694380

Conti, M., Dragoni, N., & Lesyk, V. (2016). Index IEEE communications surveys & tutorials Vol. 18. *IEEE Communications Surveys & Tutorials*, *18*(4), 3070-3086. https://doi.org/10.1109/comst.2016.2637412

Cortes-Mendoza, J. M., Tchernykh, A., Bychkov, I., Feoktistov, A., Bouvry, P., & Didelot, L. (2017). Load-aware strategies for cloud-based VoIP optimization with VM startup prediction. https://doi.org/10.1109/ipdpsw.2017.73

Cortés-Mendoza, J. M., Tchernykh, A., Drozdov, A. Y., & Didelot, L. (2016). Robust cloud VoIP scheduling under VMs startup time delay uncertainty. *Proceedings of the 9th International Conference on Utility and Cloud Computing*. https://doi.org/10.1145/2996890.3007865

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.* https://www.vitalsource.com/

Cyrillercel, M. L. (2020). Integration of a Voice Over Internet Protocol (VoIP) solution with Internet Protocol version 6 (IPv6) in an Internet Protocol Version 4 (IPv4) data network to increase employee productivity. https://doi.org/10.33774/coe-2020-m5r4b

Daoud, S., & Qu, Y. (2019). A comparison research on DSCP marking's impact to the QoS of VoIP-based and SS7-based phone calls. *2019 7th International*

Conference on Information, Communication and Networks (ICICN). https://doi.org/10.1109/icicn.2019.8834943

Deart, V., & Fatkhulin, T. (2017). Analysis of the functioning of a multi-domain transport software-defined network with controlled optical layer. *2017 21st Conference of Open Innovations Association (FRUCT)*. https://doi.org/10.23919/fruct.2017.8250168

DeLiema, M. (2017). Elder fraud and financial exploitation: Application of routine activity theory. *The Gerontologist*, *58*(4), 706-718. https://doi.org/10.1093/geront/gnw258

Delp, A. B., & Mayo, J. W. (2016). The evolution of "competition": Lessons for 21st century telecommunications policy. *Review of Industrial Organization*, *50*(4), 393-416. https://doi.org/10.1007/s11151-016-9553-9

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

Devi, G. U., Kaushik, K. V., Sreeveer, B., & Prasad, K. S. (2015). VoIP over mobile Wi-Fi hotspot. *Indian Journal of Science and Technology*, *8*(S2), 195. https://doi.org/10.17485/ijst/2015/v8is2/58751

Dey, P., & Lehner, O. (2017). Registering ideology in the creation of social entrepreneurs: Intermediary organizations, 'ideal subject,' and the promise of enjoyment. *Journal of Business Ethics: JBE, 142*(4), 753-767. https://doi.org/10.1007/s10551-016-3112-z

Dhar, S., & Chatterjee, S. (2017). A study of VOIP codecs performance over IEEE 802.11n. *2017 Devices for Integrated Circuit (DevIC)*. https://doi.org/10.1109/devic.2017.8073919

Dhillon, P. K., & Kalra, S. (2019). Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things. *Multimedia Tools and Applications*, *78*(16), 22199-22222. https://doi.org/10.1007/s11042-019-7466-y

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/

Dinar, A. E., Ghouali, S., Merzougui, R., Bentahar, A., & Merabet, B. (2020). Towards cloud transport using IP-multiservices access network (MSAN). *Journal of Optical Communications*, *0(0)*. https://doi.org/10.1515/joc-2020-0017

Dohler, M., Mahmoodi, T., Lema, M. A., Condoluci, M., Sardis, F., Antonakoglou, K., & Aghvami, H. (2017). Internet of skills, where robotics meets AI, 5G, and the tactile internet. *2017 European Conference on Networks and Communications (EuCNC)*. https://doi.org/10.1109/eucnc.2017.7980645

Drouhard, M., Chen, N.-C., Suh, J., Kocielnik, R., Pena-Araya, V., Cen, K., Xiangyi, Z., & Aragon, C. R. (2017). *Aeonium: Visual analytics to support collaborative qualitative coding*. https://doi.org/10.1109/pacificvis.2017.8031598

Dusek, G. A., Yurova, Y. V., & Ruppel, C. P. (2015). Using social media and targeted snowball sampling to survey a hard-to-reach population: A case study.

International Journal of Doctoral Studies, *10* 279-299. https://doi.org/10.28945/2296

Ebersole, C. R., Atherton, O. E., Belanger, A. L., Skulborstad, H. M., Allen, J. M., Banks, J. B., Baranski, E., Bernstein, M. J., Bonfiglio, D. B. V., Boucher, L., Brown, E. R., Budiman, N. I., Cairo, A. H., Capaldi, C. A., Chartier, C. R., Chung, J. M., Cicero, D. C., Coleman, J. A., Conway, J. G., … Nosek, B. A. (2016). Many labs 3: Evaluating participant pool quality across the academic semester via replication. *Journal of Experimental Social Psychology, 67*, 68-82. https://doi.org/10.1016/j.jesp.2015.10.012

Eck, J. E., & Madensen, T. D. (2018). Place management, Guardianship, and the Establishment of order. In *Deterrence, Choice, and Crime* (pp. 269-307). *Oxford Handbooks Online*. https://doi.org/10.1093/oxfordhb/9780190279707.013.22

Education Committee, B. (2019). Best of the best business reference web resources 2019. *Reference & User Services Quarterly*, *59*(1), 66. https://doi.org/10.5860/rusq.59.1.7225

Efimov, V. V., Mescheryakov, S. V., & Shchemelinin, D. A. (2017). Integration data model for continuous service delivery in cloud computing system. *Communications in Computer and Information Science*, 87-97. https://doi.org/10.1007/978-3-319-66836-9_8

El Kafhali, S., & Hanini, M. (2017). Stochastic modeling and analysis of feedback control on the QoS VoIP traffic in a single cell IEEE 802. 16e Networks. *IAENG International Journal of Computer Science*, 44(1), 19-28. http://www.iaeng.org

Elluri, L., Nagar, A., & Joshi, K. P. (2018). An integrated knowledge graph to automate GDPR and PCI DSS compliance. *2018 IEEE International Conference on Big Data (Big Data)*. https://doi.org/10.1109/bigdata.2018.8622236

Elmes, M., & Barry, D. (2017). Strategy retold: Toward a narrative view of strategic discourse. In *The aesthetic turn in management* (pp. 39-62). https://doi.org/10.4324/9781351147965-3

Emmert-Streib, F., Moutari, S., & Dehmer, M. (2016). The process of analyzing data is the emergent feature of data science. *Frontiers in Genetics*, *7*. https://doi.org/10.3389/fgene.2016.00012

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

Erwin, E., Gendin, S., & Kleiman, L. (Eds.). (2015). *Ethical issues in scientific research: An anthology* (Vol. 814). Routledge. https://doi.org/10.4324/9780203765135

Estepa, A., Estepa, R., Mayor, V., Madinabeitia, G., & Davis, M. (2018). Adaptative control of packetization to improve the energy efficiency of VoIP applications in IEEE 802.11 networks. *Network Protocols and Algorithms*, *9*(3-4), 115. https://doi.org/10.5296/npa.v9i3-4.12308

Eterovic-Soric, B., Choo, K. R., Ashman, H., & Mubarak, S. (2017). Stalking the stalkers – detecting and deterring stalking behaviors using technology: A review. *Computers & Security*, *70*, 278-289. https://doi.org/10.1016/j.cose.2017.06.008

Etikan, I. (2017). Sampling and sampling methods. *Biometrics & Biostatistics International Journal*, *5*(6). https://doi.org/10.15406/bbij.2017.05.00149

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1-4. https://doi.org/10.11648/j.ajtas.20160501.11

Evans, D. R., Hearn, M. T., Uhlemann, M. R., & Ivey, A. E. (2017). *Essential interviewing: A programmed approach to effective communication*. Nelson Education. https://www.abebooks.com/

Evens, T., & Donders, K. (2016). Mergers and acquisitions in TV broadcasting and distribution: Challenges for competition, industrial, and media policy. *Telematics and Informatics*, *33*(2), 674-682. https://doi.org/10.1016/j.tele.2015.04.003

Fatehi, K., & Choi, J. (2018). International information systems management. *Springer Texts in Business and Economics*, 309-338. https://doi.org/10.1007/978-3-319-96622-9_10

Fayyaz, Y., Khan, D. M., Fayyaz, F., Qadri, S., Naweed, S., & Fahad, M. (2016). The Evaluation of voice-over-internet protocol (VoIP) by means of Trixbox. *International Journal of Natural and Engineering Sciences (IJNES) E-ISSN: 2146-0086*, *7*(3), 33-41. https://www.researchgate.net/

Fischer, G., Fogli, D., & Piccinno, A. (2017). Revisiting and broadening the meta-design framework for end-user development. *New Perspectives in End-User Development*, 61-97. https://doi.org/10.1007/978-3-319-60291-2_4

Frieden, R. (2019). An introduction to data property ownership rights and data protection responsibilities. *SSRN Electronic Journal*. http://doi.org/10.2139/ssrn.3432422

Furchtgott-Roth, H. (2017). The unvanquished: The administrative state and the federal communications commission. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3127005

Furnell, S. (2020). Technology use, abuse, and public perceptions of cybercrime. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 45-66. https://doi.org/10.1007/978-3-319-78440-3_9

Fusch, P., & Ness, L. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, 20(9), 1408-1416. https://doi.org/10.46743/2160-3715/2015.2281

Gandotra, R., & Perigo, L. (2020). VoIP—A software-defined VoIP framework for SIP and dynamic QoS. *The Computer Journal*, *64*(2), 254-263. https://doi.org/10.1093/comjnl/bxaa152

Ganesan, V., & MSK, M. (2017). A secured load mitigation and distribution scheme for securing SIP server. *Security and Communication Networks*, *2017*, 1-14. https://doi.org/10.1155/2017/7821487

Garth, M., Millet, A., Shearer, E., Stafford, S., Bereknyei Merrell, S., Bruce, J., Schillinger, E., Aaronson, A., & Svec, D. (2017). Inter professional collaboration: A qualitative study of non-physician perspectives on resident competency. *Journal of General Internal Medicine*, *33*(4), 487-492. https://doi.org/10.1007/s11606-017-4238-0

Gaur, A., & Kumar, M. (2018). A systematic approach to conducting review studies: An assessment of content analysis in 25 years of IB research. *Journal of World Business*, *53*(2), 280-289. https://doi.org/10.1016/j.jwb.2017.11.003

Gavilanez, O., Gavilanez, F., & Rodriguez, G. (2017). Audit analysis models, Security frameworks, and their relevance for VoIP. *arXiv preprint arXiv:1704.02440*. https://arxiv.org/pdf/1704.02440.pdf

Geneiatakis, D., Kambourakis, G., & Lambrinoudakis, C. (2018). SIP security: threats, vulnerabilities and countermeasures. *SIP Handbook: Services, Technologies, and Security of Session Initiation Protocol*. https://doi.org/10.1201/9781315218939-28

Gentles, S. J., Charles, C., Nicholas, D. B., Ploeg, J., & McKibbon, K. A. (2016). Reviewing the research methods literature: Principles and strategies illustrated by a systematic overview of sampling in qualitative research. *Systematic Reviews*, *5*(1). https://doi.org/10.1186/s13643-016-0343-0

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/

Ghalut, T., Larijani, H., & Shahrabi, A. (2016). QoE-aware optimization of video stream downlink scheduling over LTE networks using RNNs and genetic algorithm. *Procedia Computer Science*, *94*, 232-239. https://doi.org/10.1016/j.procs.2016.08.036

Ghazali, A. J., Al-Nuaimy, W., Al-Ataby, A., & Al-Taee, M. A. (2016). Building IPv6 based tunneling mechanisms for VoIP security. *2016 13th International Multi-Conference on Systems, Signals & Devices (SSD)*. https://doi.org/10.1109/ssd.2016.7473737

Giorgini, V., Mecca, J. T., Gibson, C., Medeiros, K., Mumford, M. D., Connelly, S., & Devenport, L. D. (2015). Researcher perceptions of ethical guidelines and codes of conduct. *Accountability in Research*, *22*(3), 123-138. https://doi.org/10.1080/08989621.2014.955607

Goodman-Deane, J., Mieczakowski, A., Johnson, D., Goldhaber, T., & Clarkson, P. J. (2016). The impact of communication technologies on life and relationship satisfaction. *Computers in Human Behavior*, *57*, 219-229. https://doi.org/10.1016/j.chb.2015.11.053

Gorard, S. (2015). Rethinking 'quantitative' methods and the development of new researchers. *Review of Education*, *3*(1), 72-96. https://doi.org/10.1002/rev3.3041

Guidry, K. M. (2019). Carpenter v. United States: A step further in privacy protection but not far enough. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3334588

Gupta, A., & Jha, R. K. (2015). Security threats of wireless networks: A survey. *International Conference on Computing, Communication & Automation*. https://doi.org/10.1109/ccaa.2015.7148407

Gurrapu, S., Mehta, S., & Panbude, S. (2016). Comparative study for performance analysis of VOIP codecs over WLAN in nonmobility scenarios. *International*

Journal of Information Technology, Modeling, and Computing, *4*(4), 01-16. https://doi.org/10.5121/ijitmc.*2016*.4401

Hadi, M. A., & Closs, S. J. (2016). Ensuring rigor and trustworthiness of qualitative research in clinical pharmacy. *International Journal of Clinical Pharmacy*, *38*(3), 641-646. https://doi.org/10.1007/s11096-015-0237-6

Haggag, M. H. (2017). Social engineering attacks detection techniques: Survey study. *International Journal of Engineering and Computer Science*. https://doi.org/10.18535/ijecs/v6i1.09

Harnack, K., & Talbot, J. (2017). Telephone network interfacing. *National Association of Broadcasters Engineering Handbook*, 371-398. https://doi.org/10.4324/9781315680149-24

Hasan, M. Z., & Hussain, M. Z. (2017). Collective study on security threats in VOIP networks. *International Journal of Scientific and Technology Research*, *6*(01). https://doi.org/10.18535/ijecs/v6i1.09

Hawdon, J., Costello, M., Barrett-Fox, R., & Bernatzky, C. (2019). The perpetuation of online hate: A Criminological analysis of factors associated with participating in an online attack. *Journal of Hate Studies*, *15*(1), 157. https://doi.org/10.33972/jhs.166

Hawdon, J., Costello, M., Ratliff, T., Hall, L., & Middleton, J. (2017). Conflict management styles and cyber victimization: Extending routine activity theory. *Sociological Spectrum*, *37*(4), 250-266. https://doi.org/10.1080/02732173.2017.1334608

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence-Based Nursing*, *18*(3), 66-67. https://doi.org/10.1136/eb-2015-102129

Heidt, C. T., Arbuthnott, K. D., & Price, H. L. (2016). The effects of distributed learning on enhanced cognitive interview training. *Psychiatry, Psychology and Law*, *23*(1), 47-61. https://doi.org/10.1080/13218719.2015.1032950

Hephzibah, I. A., & Oludare, F. O. (2015). *Modelling and simulation of Voice Over Internet Protocol (VoIP) over Wireless Local Area Network (WLAN).* http://www.ijstr.org

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). Victims of personal crime: An empirical foundation for a theory of personal victimization: An empirical foundation for a theory of personal victimization. https://www.ncjrs.gov

Hogan, T., Hinrichs, U., & Hornecker, E. (2016). The elicitation interview technique: Capturing people's experiences of data representations. *IEEE Transactions on Visualization and Computer Graphics*, 22(12), 2579-2593. https://doi.org/10.2307/2066613

Holub, J., Wallbaum, M., Smith, N., & Avetisyan, H. (2018). Analysis of the dependency of call duration on the Quality of VoIP calls. *IEEE Wireless Communications Letters*, *7*(4), 638-641. https://doi.org/10.1109/lwc.2018.2806442

Hopkins, R. M., Regehr, G., & Pratt, D. D. (2016). A framework for negotiating positionality in phenomenological research. *Medical Teacher*, *39*(1), 20-25. https://doi.org/10.1080/0142159x.2017.1245854

Hsieh, W., & Leu, J. (2017). Implementing a secure VoIP communication over SIP-based networks. *Wireless Networks*, *24*(8), 2915-2926. https://doi.org/10.1007/s11276-017-1512-3

Hu, Z., Yan, H., Yan, T., Geng, H., & Liu, G. (2020). Evaluating QoE in VoIP networks with QoS mapping and machine learning algorithms. *Neurocomputing*, *386*, 63-83. https://doi.org/10.1016/j.neucom.2019.12.072

Huang, T. H., Yu, C., & Kao, H. (2017). Data-driven and deep learning methodology for deceptive advertising and phone scams detection. *2017 Conference on Technologies and Applications of Artificial Intelligence (TAAI)*. https://doi.org/10.1109/taai.2017.30

Hussain, I., Djahel, S., Zhang, Z., & Naït-Abdesselam, F. (2015). A comprehensive study of flooding attack consequences and countermeasures in session initiation protocol (sip). *Security and Communication Networks*, *8*(18), 4436-4451. https://doi.org/10.1002/sec.1328

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, 1-12. https://doi.org/10.1080/08874417.2019.1650676

Ibrahim, H. (2019). Improving quality of service for internet protocol television and voice over internet protocol over long term evolution networks. *International Journal of Communication Networks and Distributed Systems*, *22*(4), 1. https://doi.org/10.1504/ijcnds.2019.10016428

Ibrahim, N., & Edgley, A. (2015). Embedding researcher’s reflexive accounts within the analysis of a semi-structured qualitative interview. *The Qualitative Report*, *20*(10), 1671-1681. https://nsuworks.nova.edu

Idom, A. M., & Tormusa, D. O. (2016). Causes, types, and likely victims of cybercrimes in selected higher institutions, South-South, Nigeria. *FULafia Journal of Social Sciences, 1 (1): 202, 218.* http://www.fulafiajst.com/

Imran, A., & Yusoff, R. M. (2015). Empirical validation of qualitative data: A mixed-method approach. *International Journal of Economics and Financial Issues*, *5*(1S), 389-396. https://www.econjournals.com/

Irshad, A., Sher, M., Rehman, E., Ch, S. A., Hassan, M. U., & Ghani, A. (2015). A single round-trip sip authentication scheme for voice over internet protocol using smart card. *Multimedia Tools and Applications*, *74*(11), 3967-3984. https://doi.org/10.1007/s11042-015-2988-4

Ivy, B. P. U., & Priya, M. A. (2018). Detection and prevention of distributed denial of service attacks in VoIP. *Swansea Printing Technology LTD*, 1985-2000. http://www.tagajournal.com/gallery/v14.183.pdf

Jacobson, I., Spence, I., & Ng, P. (2017). Is there a single method for the internet of things? *Communications of the ACM*, *60*(11), 46-53. https://doi.org/10.1145/3106637

Jagosh, J., Bush, P. L., Salsberg, J., Macaulay, A. C., Greenhalgh, T., Wong, G., Cargo, M., Green, L. W., Herbert, C. P., & Pluye, P. (2015). A realist evaluation of community-based participatory research: partnership synergy, trust building and related ripple effects. *BMC Public Health, 15*(1). https://doi.org/10.1186/s12889-015-1949-1

Jalendry, S., & Verma, S. (2015). A detail review on voice over internet protocol (VoIP). *International Journal of Engineering Trends and Technology (IJETT)*, *ISSN, 2231-5381.* http://www.ijettjournal.org/

Jan, S. U., & Qayum, F. (2017). An improved lightweight privacy-preserving authentication scheme for SIP-based-VoIP using smart card. *SSRN Electronic Journal*. Volume 2 issue 3. https://doi.org/10.2139/ssrn.3345110

Javed, I. T., Toumi, K., Alharbi, F., Margaria, T., & Crespi, N. (2021). Detecting nuisance calls over internet telephony using caller reputation. *Electronics*, *10*(3), 353. https://doi.org/10.3390/electronics10030353

Jingi, A. M., & Muhammad, M. (2017). VoIP security: Common attacks and their countermeasures. *International Journal of Computer Science and Information Security, 15*(3), 421-428. https://www.ijcsis.org

Johnson, S., Ferreira, J., Mendes, A., & Cordry, J. (2019). Lost in disclosure: On the inference of password composition policies. *2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*. https://doi.org/10.1109/issrew.2019.00082

Joslin, R., & Müller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. *International Journal of Project Management*, *34*(6), 1043-1056. https://doi.org/10.1016/j.ijproman.2016.05.005

Kabir, S. (2017). An overview of fault tree analysis and its application in model-based dependability analysis. *Expert Systems with Applications*, *77*, 114-135. https://doi.org10.1016/j.eswa.2017.01.058

Kallio, H., Pietilä, A. M., 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.org/10.1111/jan.13031

Kalu, F. A. (2017). What makes qualitative research good research? An exploratory analysis of critical elements. *International Journal of Social Science Research*, *5*(2), 43. https://doi.org/10.5296/ijssr.v5i2.10711

Karakus, M., & Durresi, A. (2017). A survey: Control plane scalability issues and approaches in software-defined networking (SDN). *Computer Networks*, *112*, 279-293. https://doi.orf/10.1016/j.comnet.2016.11.017

Kass, N. E., Taylor, H. A., Ali, J., Hallez, K., & Chaisson, L. (2015). A pilot study of simple interventions to improve informed consent in clinical research: feasibility, approach, and results. *Clinical Trials*, *12*(1), 54-66. https://doi.org/10.1177/1740774514560831

Kaul, S., & Jain, A. (2019). Opus and session initiation protocol security in voice over IP (VOIP). *European Journal of Engineering Research and Science*, *4*(12), 27-37. https://doi.org/10.24018/ejers.2019.4.12.1625

Kaur, G., Kaur, J., Aggarwal, S., Singla, C., Mahajan, N., Kaushal, S., & Sangaiah, A. K. (2017). An optimized hardware calibration technique for transmission of real-time applications in VoIP network. *Multimedia Tools and Applications*, *78*(5), 5537-5570. https://doi.org/10.1007/s11042-017-5203-y

Kfoury, E. F., & Khoury, D. J. (2018). Secure end-to-end VoIP system based on Ethereum blockchain. *Journal of Communications*, 450-455. https://doi.org/10.12720/jcm.13.8.450-455

Khudhur, F. H., Saddy, S. M., & Jabbar, M. (2018). Investigation of the Quality of Service for VOIP traffic signaling protocol using simulation-based approach. *Journal of Computer Engineering & Information Technology*, *07*(02). https://doi.org/10.4172/2324-9307.1000197

Kim, H., Sefcik, J. S., & Bradway, C. (2016). Characteristics of qualitative descriptive studies: A systematic review. *Research in Nursing & Health*, *40*(1), 23-42. https://doi.org/10.1002/nur.21768

Kim, K., Kim, T., Nam-Wook, C., & Kim, M. (2015). Toll fraud detection of VoIP service networks in ubiquitous computing environments. *International Journal of Distributed Sensor Networks, Volume 11 issue 9.* https://doi.org/10.1155/2015/276408

Kizza, J. M. (2017). Computer network security protocols. *Guide to Computer Network Security*, 365-396. https://doi.org/10.1007/978-3-319-55606-2_17

Kolhar, M., Alameen, A., & Gulam, M. (2017). Performance evaluation of framework of VoIP/SIP server under virtualization environment along with the most common security threats. *Neural Computing and Applications*, *30*(9), 2873-2881. https://doi.org/10.1007/s00521-017-2886-y

Korstjens, I., & Moser, A. (2017). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120-124. https://doi.org/10.1080/13814788.2017.1375092

Kozleski, E. B. (2017). The uses of qualitative research. *Research and Practice for Persons with Severe Disabilities*, *42*(1), 19-32. https://doi.org/10.1177/1540796916683710

Kumar, V., & Roy, O. P. (2020). Reliability and security analysis of VoIP communication systems. *Rising Threats in Expert Applications and Solutions*, 687-693. https://doi.org/10.1007/978-981-15-6014-9_84

Kurt, B., Yıldız, Ç., Ceritli, T. Y., Sankur, B., & Cemgil, A. T. (2018). A Bayesian change point model for detecting SIP-based DDoS attacks. *Digital Signal Processing*, *77*, 48-62. https://doi.org/10.1016/j.dsp.2017.10.009

Laghrissi, A., & Taleb, T. (2019). A survey on the placement of virtual resources and virtual network functions. *IEEE Communications Surveys & Tutorials*, *21*(2), 1409-1434. https://doi.org/10.1109/comst.2018.2884835

Laumann, K. (2018). Criteria for qualitative methods in human reliability analysis. *Reliability Engineering & System Safety*. https://doi.org/10.1016/j.ress.2018.07.001

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37, 263-280. https://doi.org/10.1080/01639625.2015.1012409

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324-327. https://doi.org/10.4103/2249-4863.161306

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, *16*(4), 473-475. https://doi.org/10.1177/1524839915580941

Li, H., Xu, X., Liu, C., Ren, T., Wu, K., Cao, X., Zhang, W., Yu, Y., & Song, D. (2018). A machine learning approach to prevent malicious calls over telephony networks. https://doi.org/10.1109/sp.2018.00034

Li, T., Zeng, C., Jiang, Y., Zhou, W., Tang, L., Liu, Z., & Huang, Y. (2017). Data-driven techniques in computing system management. *ACM Computing Surveys*, *50*(3), 1-43. https://doi.org/10.1145/3092697

Llinares, F. M. (2015). That cyber routine, that cyber victimization: Profiling victims of cybercrime. In *Cybercrime Risks and Responses* (pp. 47-63). https://doi.org/10.1057/9781137474162_2

Madill, A., & Sullivan, P. (2018). Mirrors, portraits, and member checking: Managing difficult moments of knowledge exchange in the social sciences. *Qualitative Psychology*, *5*(3), 321-339. https://doi.org/10.1037/qup0000089

Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, *13(12*), https://doi.org/10.1177/1550147717741463

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2019). Anatomy of threats to the Internet of things. *IEEE Communications Surveys & Tutorials*, *21*(2), 1636-1675. https://doi.org/10.1109/comst.2018.2874978

Malik, J. K., & Choudhury, S. (2019). A brief review on cybercrime-growth and evolution. *Pramana Research Journal*, *9*(3), 242. https://www.pramanaresearch.org/gallery/prj-p580.pdf

Malisuwan, S., Milindavanij, D., & Kaewphanuekrungsi, W. (2016). Quality of service (QoS) and quality of experience (QoE) of the 4G LTE perspective. *International Journal of Future Computer and Communication*, *5*(3), 158-162. https://doi.org/10.18178/ijfcc.2016.5.3.463

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies. *Qualitative Health Research*, *26*(13), 1753-1760. https://doi.org/10.1177/1049732315617444

Manne, G., Morris, J., Stout, K., & Auer, D. (2018). FTC hearings on competition & Consumer protection in the 21st century, FTC docket no. FTC-2018-0091, comments of the international center for law & economics on the consumer welfare standard (Hearing No. 5). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3384363

Manzano, A. (2016). The craft of interviewing in realist evaluation. *Evaluation*, *22*(3), 342-360. https://doi.org/10.1177/1356389016638615

Marland, A., & Esselment, A. L. (2018). Negotiating with gatekeepers to get interviews with politicians: Qualitative research recruitment in a digital media environment. *Qualitative Research*, *19*(6), 685-702. https://doi.org/10.1177/1468794118803022

Mason, J. (2017). *Qualitative researching*. *Thousand Oaks, CA:* SAGE. https://uk.sagepub.com/en-gb/eur/qualitative-researching/book244365#reviews

Matua, G. A. (2015). Choosing phenomenology as a guiding philosophy for nursing research. *Nurse Researcher*, *22*(4), 30-34. https://doi.org/10.7748/nr.22.4.30.e1325

Mazhar, M. H., & Shafiq, Z. (2018). Real-time video quality of experience monitoring for HTTPS and QUIC. *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. https://doi.org/10.1109/infocom.2018.8486321

McGuirk, P. M., & O'Neill, P. (2016). Using questionnaires in qualitative human geography. In I. Hay (Eds.), *Qualitative* Research *Methods in Human Geography (pp. 246-273). Don Mills, Canada:* Oxford University Press. https://ro.uow.edu.au/sspapers/2518

McInnes, N., & Wills, G. (2021). The VoIP PBX honeypot advance persistent threat analysis. *Proceedings of the 6th International Conference on Internet of Things, Big Data and Security*. https://doi.org/10.5220/0010443500700080

McInnes, N., Zaluska, E., & Wills, G. (2019). Analysis of a PBX toll fraud honeypot. *International Journal for Information Security Research*, *9*(1), 821-830. https://doi.org/10.20533/ijisr.2042.4639.2019.0094

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

McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice*, *31*(1), 30-52. https://doi.org/10.1177/1043986214552607

McQuade, S. (1998). *Towards a theory of technology enabled crime.* Unpublished manuscript. George Mason University, Fairfax, Virginia. http://citeseerx.ist.psu.edu/

McQuade, S. (2001). Technology-enabled crime, policing and security. *The Journal of Technology Studies*, *32*(1). https://doi.org/10.21061/jots.v32i1.a.5

Meghani, Z. (2017). Regulations of consumer products. *Consumer Perception of Product Risks and Benefits*, 495-513. https://doi.org/10.1007/978-3-319-50530-5_26

Merien, T., Brosset, D., Bellekens, X., & Claramunt, C. (2018). A human-centred model for network flow analysis. *2018 2nd Cyber Security in Networking Conference* (CSNet) https://doi.org/10.1109/csnet.2018.8602913

Miethe, T. D., & Meier, R. F. (1990). Opportunity, choice, and criminal victimization rates: A theory of a theoretical model. *Journal of Research in Crime & Delinquency, 27*, 243-266. https://doi.org/10.1177/0022427890027003003

Milzcik, E. (2015). Routine activities theory as a predictor of cybercrime victimization (Order No. 1593781).

Miraz, M. H., Ganie, M. A., Ali, M., Molvi, S. A., & Hussein, A. H. (2015). Performance evaluation of VoIP QoS parameters using WiFi-UMTS networks. *Transactions on Engineering Technologies*, 547-561. https://doi.org/10.1007/978-94-017-9804-4_38

Miraz, M. H., Molvi, S. A., Ganie, M. A., Ali, M., & Hussein, A. H. (2017). Simulation and analysis of quality of service (QoS) parameters of voice over IP (VoIP) traffic through heterogeneous networks. *International Journal of Advanced Computer Science and Applications*, *8*(7). https://doi.oeg/10.14569/ijacsa.2017.080732

Moffitt, K., Karabiyik, U., Hutchinson, S., & Yoon, Y. H. (2021). Discord forensics: The logs keep growing. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*. https://doi.org/10.1109/ccwc51732.2021.9376133

Montazerolghaem, A., Shekofteh, S., Yaghmaee, M., & Naghibzadeh, M. (2017). A load scheduler for SIP proxy servers: Design, implementation, and evaluation of a history weighted window approach. *International Journal of Communication Systems*, *30*(3), e2980. https://doi.org/10.1002/dac.2980

Moore, E., & Llompart, J. (2017). Collecting, transcribing, analyzing, and presenting plurilingual interactional data. *Qualitative approaches to research on plurilingual education / Enfocaments qualitatius per a la recerca en educació plurilingüe / Enfoques cualitativos para la investigación en educación plurilingüe*, 403-417. https://doi./10.14705/rpnet. 2017.emmd2016.638

Mousavi, S. M., & St-Hilaire, M. (2015). Early detection of DDoS attacks against SDN controllers. *2015 International Conference on Computing, Networking and Communications (ICNC)*. https://doi.org/10.1109/iccnc.2015.7069319

Muelas, D., Lopez de Vergara, J. E., Ramos, J., Garcia-Dorado, J. L., & Aracil, J. (2017). On the impact of TCP segmentation: Experience in VoIP monitoring. *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. https://doi.org/10.23919/inm.2017.7987363

Naeem, M. M., Hussain, I., & Saad Missen, M. M. (2020). A survey on registration hijacking attack consequences and protection for session initiation protocol (SIP). *Computer Networks*, *175*, 107250. https://doi.org/10.1016/j.comnet.2020.107250

Nastase, L. (2017). Security in the internet of things: A survey on application layer protocols. *2017 21st International Conference on Control Systems and Computer Science (CSCS)*. https://doi.org/10.1109/cscs.2017.101

Nazih, W., Elkilani, W. S., Dhahri, H., & Abdelkader, T. (2020). Survey of countering dos/DDoS attacks on SIP based VoIP networks. *Electronics*, *9*(11), 1827. https://doi.org/10.3390/electronics9111827

Neacsu, E., & Schiopu, P. (2020). An analysis of security threats in VoIP communication systems. *2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. https://doi.org/10.1109/ecai50035.2020.9223162

Neale, J. (2016). Iterative categorization (IC): A systematic technique for analyzing qualitative data. *Addiction*, *111*(6), 1096-1106. https://doi.org/10.1111/add.13314

Nebeker, C., Lagare, T., Takemoto, M., Lewars, B., Crist, K., Bloss, C. S., & Kerr, J. (2016). Engaging research participants to inform the ethical conduct of mobile imaging, pervasive sensing, and location tracking research. *Translational Behavioral Medicine, 6*(4), 577-586. https://doi.org/10.1007/s13142-016-0426-4

Neupane, K., Haddad, R., & Chen, L. (2018). Next-generation firewall for network security: A survey. *SoutheastCon 2018*. https://doi.org/10.1109/secon.2018.8478973

Noh, H., Song, Y., & Lee, S. (2016). Identifying emerging core technologies for the future: Case study of patents published by leading telecommunication organizations. *Telecommunications Policy*, *40*(10-11), 956-970. https://doi.org/10.1016/j.telpol.2016.04.003

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

Ntantogian, C., Veroni, E., Karopoulos, G., & Xenakis, C. (2019). A survey of voice and communication protection solutions against wiretapping. *Computers & Electrical Engineering*, *77*, 163-178. https://doi.org/10.1016/j.compeleceng.2019.05.008

Nuño, P., Suárez, C., Suárez, E., Bulnes, F. G., DelaCalle, F. J., & Granda, J. C. (2020). A diagnosis and hardening platform for an asterisk VoIP PBX. *Security and Communication Networks*, *2020*, 1-14. https://doi.org/10.1155/2020/8853625

Nusbaum, L., Douglas, B., Damus, K., Paasche-Orlow, M., & Estrella-Luna, N. (2017). Communicating risks and benefits in informed consent for research: A qualitative study. *Global Qualitative Nursing Research*, *4*, https://doi.org/10.1177/2333393617732017

Oh, S., Costello, K. L., Chen, A. T., & Wildemuth, B. M. (2016). Qualitative methods for studying health information behaviors. *Proceedings of the Association for Information Science and Technology*, *53*(1), 1-5. https://doi.org/10.1002/pra2.2016.14505301024

Oliveira, L., Rodrigues, J., Kozlov, S., Rabêlo, R., & Albuquerque, V. (2019). MAC layer protocols for internet of things: A survey. *Future Internet, 11*(1), 16. https://doi.org/10.3390/fi11010016

Olson, J., McAllister, C., Grinnell, L., Gehrke Walters, K., & Appunn, F. (2016). Applying constant comparative method with multiple investigators and inter-coder reliability. *The Qualitative Report*, 21(1), 26-42. https://doi.org/10.46743/2160-3715/2016.2447

Oltmann, S. M. (2016). Qualitative interviews: A methodological discussion of the interviewer and respondent contexts. *In forum: Qualitative Social Research (Vol. 17, No. 2, p. 1).* http://www.qualitative-research.net

Oo, T. T., & De La Salle University, Manila. (2019). Design and Implementation of Bandwidth Monitoring, Line Aggregation of VoIP. *International Journal of Advanced Trends in Computer Science and Engineering*, 1326-1331. https://doi.org/10.30534/ijatcse/2019/46842019

Oppitz, M., & Tomsu, P. (2017). Networks for sharing and connecting. *Inventing the Cloud Century*, 97-129. https://doi.org/10.1007/978-3-319-61161-7_5

Ose, S. O. (2016). Using Excel and Word to structure qualitative data. *Journal of Applied Social Science*, *10*(2), 147-162. https://doi.org/10.1177/1936724416664948

Packer, J., & Reuschel, W. (2018). VoIP accessibility: A usability study of voice over internet protocol (VoIP) systems and a survey of VoIP users with vision loss. *Journal of Visual Impairment & Blindness*, *112*(1), 47-60. https://doi.org/10.1177/0145482x1811200105

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*(5), 533-544. https://doi.org/10.1007/s10488-013-0528-y

Park, N. (2007). User acceptance of computer-based VoIP phone service: An application of the technology acceptance model (Doctoral Dissertation).

Patel, M. M. (2016). Performance and security in VOIP (Doctoral Dissertation).

Payne, B. R., & Abegaz, T. T. (2017). Securing the Internet of things: Best practices for deploying IoT devices. *Computer and Network Security Essentials*, 493-506. https://doi.org/10.1007/978-3-319-58424-9_28

Peha, J. M. (2016). Encryption cannot protect consumer privacy from Isps. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2806698

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

Perkins, C., & Singh, V. (2017). *Multimedia congestion control: Circuit breakers for unicast RTP sessions. ISSN: 2070-1721.* https://doi.org/10.17487/rfc8083

Perwej, Y. (2017). The next generation of wireless communication using Li-Fi (Light Fidelity) technology. *Journal of Computer Networks*, *4*(1), 20-29. https://doi.org/10.12691/jcn-4-1-3

Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? *Aggression and Violent Behavior*, *34*, 193-200. https://doi.org/10.1016/j.avb.2017.01.012

Petrie, K. (2016). Coming unstuck as an interviewer. *Waikato Journal of Education*, *11*(1). https://doi.org/10.15663/wje.v11i1.322

Ponelis, S. (2015). Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of information systems research in small and medium enterprises. *International Journal of Doctoral Studies*, *10*, 535-550. https://doi.org/10.28945/2339

Popping, R. (2015). Analyzing open-ended questions by means of text analysis procedures. *Bulletin of Sociological Methodology/Bulletin de Méthodologie Sociologique*, *128*(1), 23-39. https://doi.org/10.1177/0759106315597389

Prachi. (2021). Detection of Botnet based attacks on network. *Research Anthology on Combating Denial-of-Service Attacks*, 74-88. https://doi.org/10.4018/978-1-7998-5348-0.ch004

Praseed, A., & Thilagam, P. S. (2019). DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications. *IEEE Communications Surveys & Tutorials*, *21*(1), 661-685. https://doi.org/10.1109/comst.2018.2870658

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and routine activity theories Revisited: The importance of "risk" to the study of victimization. *Victims & Offenders*, *11*(3), 335-354. https://doi.org/10.1080/15564886.2015.1057351

Quamara, M., & Gupta, B. B. (2018). Role of software-defined networking (SDN) in Internet of things (IoT) security: Attacks and countermeasures. *Computer and Cyber Security*, 557-589. https://doi.org/10.1201/9780429424878-21

Radcliffe, D., Furey, E., & Blue, J. (2019). An SD-WAN solution assuring business quality VoIP communication for home based employees. *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)*. https://doi.org10.1109/smartnets48225.2019.9069755

Rahaman, S., Wang, G., & Yao, D. D. (2019). Security certification in payment card industry. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/3319535.3363195

Raheja, T., & Munjal, D. (2015). A comprehensive survey on voice over internet protocol (VoIP). *International Journal of Advanced Research in Computer Engineering & Technology (IJARCT),* vol, 4, 1552-1557. http://www.ijarcet.org

Rahman, M. M., Shahiduzzaman, K. M., Karmaker, B. K., & Khan, M. M. H. (2017). VoIP on IP PBX system using secure VPN communication and delay analysis. *IOSR Journal of Electronics and Communication Engineering, 12*(02), 12-19. https://doi.org/10.9790/2834-1202021219

Rajput, M. T. S., & Barkatullah University Institute of Technology Bhopal, India. (2017). VoIP packet analyzer for detecting hreats in SIP network. *International Journal of Advanced Research in Computer Science*, *8*(9), 613-618. https://doi.org/10.26483/ijarcs.v8i9.5167

Ramachandran, M. (2019). Enterprise security framework for enterprise cloud data centres. *Cloud Security*, 226-248. https://doi.org/10.4018/978-1-5225-8176-5.ch010

Rani, S., Ahmed, S. H., Talwar, R., Malhotra, J., & Song, H. (2017). IoMT: A reliable cross layer protocol for internet of multimedia things. *IEEE Internet of Things Journal*, *4*(3), 832-839. https://doi./10.1109/jiot.2017.2671460

Ranney, M. L., Meisel, Z. F., Choo, E. K., Garro, A. C., Sasson, C., & Morrow Guthrie, K. (2015). Interview-based qualitative research in emergency care part II: Data collection, analysis, and results reporting. *Academic Emergency Medicine*, *22*(9), 1103-1112. https://doi./10.1111/acem.12735

Ravindranath, R., Ravindran, P., & Kyzivat, P. (2017). Session initiation protocol (SIP) recording call flows. https://doi.org/10.17487/rfc8068

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119-1139. https://doi.org/10.1177/0306624x15572861

Reyns, B. W., Henson, B., & Fisher, B. S. (2015). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice, 32*, 148-168. https://doi.org/10.1177/1043986215621378

Rither, A. C., & Hoxie, C. M. (2017). Legal considerations of cyber-physical systems and the Internet of things. *Security and Privacy in Cyber-Physical Systems*, 93-115. https://doi.org/10.1002/9781119226079.ch5

Rojas, H., Renteria, R., Luque, E. N., Peralta, M., & Merma, J. L. (2018). Proposal to implement low-cost digital communication using VoIP technology, a case study. *International Journal of Future Computer and Communication*, *7*(3), 68-73. https://doi.org/10.18178/ijfcc.2018.7.3.523

Rosenberg, J. M., & Koehler, M. J. (2015). Context and technological pedagogical content knowledge (TPACK): A systematic review. *Journal of Research on Technology in Education, 47*, 186–210. https://doi.org/10.1080/15391523.2015.1052663

Roulston, K., & Shelton, S. A. (2015). Reconceptualizing bias in teaching qualitative research methods. *Qualitative Inquiry*, *21*(4), 332-342. https://doi.org/10.1177/1077800414563803

Roy, A., Acharya, T., & DasBit, S. (2018). Quality of service in delay tolerant networks: A survey. *Computer Networks*, *130*, 121-133. https://doi.org/10.1016/j.comnet.2017.11.010

Roy, O. P., & Kumar, V. (2021). A survey on voice over internet protocol (VoIP) reliability research. *IOP Conference Series: Materials Science and Engineering*, *1020*, 012015. https://doi.org/10.1088/1757-899x/1020/1/012015

Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers & Security*, *87*, 101561. https://doi.org/10.1016/j.cose.2019.06.015

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016). Cybercriminals, cyberattacks, and cybercrime. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*. https://doi.org/10.1109/icccf.2016.7740434

Safoine, R., Mounir, S., & Farchi, A. (2018). Comparative study on DOS attacks detection techniques in SIP-based VOIP networks. *2018 6th International Conference on Multimedia Computing and Systems (ICMCS)*. https://doi.org/10.1109/icmcs.2018.8525878

Sahin, M., Francillon, A., Gupta, P., & Ahamad, M. (2017). SoK: Fraud in telephony networks. *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. https://doi.org/10.1109/eurosp.2017.40

Saidat, M. R. (2019). A design of an enhanced redundant SIP model for securing SIP-based networks. *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*. https://doi.org/10.1109/aiccsa47632.2019.9035304

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Salamzadeh, A., Arasti, Z., & Elyasi, G. M. (2017). Creation of ICT-based social start-ups in Iran: A Multiple Case Study. *Journal of Enterprising Culture*, *25*(01), 97-122. https://doi.org/10.1142/s0218495817500042

Sasikala, B. (2017). Internet of things: A survey on security issues analysis and countermeasures. *International Journal of Engineering and Computer Science*. https://doi.org/10.18535/ijecs/v6i5.41

Satapathy, A., & Livingston, L. J. (2016). A comprehensive survey of security issues and defense framework for VoIP cloud. *Indian Journal of Science and Technology*, *9*(6). https://doi.org/10.17485/ijst/2016/v9i6/81980

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

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1460. https://doi.org/10.3390/electronics9091460

Schaefer, L. (2021). Routine activity theory. *Oxford Research Encyclopedia of Criminology and Criminal Justice*. https://doi.org/10.1093/acrefore/9780190264079.013.326

Schaefer, L., & Mazerolle, L. (2017). Putting process into routine activity theory: Variations in the control of crime opportunities. *Security Journal*, *30*(1), 266-289. https://doi.org/10.1057/sj.2015.39

Seaman, J. (2021). Information systems security. *Protective Security*, 323-355. https://doi.org/10.1007/978-1-4842-6908-4_8

Semerci, M., Cemgil, A. T., & Sankur, B. (2018). An intelligent cybersecurity system against DDoS attacks in SIP networks. *Computer Networks*, *136*, 137-154. https://doi.org/10.1016/j.comnet.2018.02.025

Shaffer, G. (2017). A critical discourse analysis of how the telecommunications industry influenced VoIP deregulation legislation in 36 states. *First Monday*, *23*(1). https://doi.org/10.5210/fm.v23i1.8142

Shaw, U., & Sharma, B. (2016). A survey paper on voice over internet protocol (VOIP). *International Journal of Computer Applications*, *139*(2), 16-22. https://doi.org/10.5120/ijca2016909112

Shoket, H., & Aulakh, J. S. (2018). Secure VoIP LTE network for secure transmission using PLRT (Packet Level Restraining Technique) under DDOS attack. *2018 5th*

International Conference on Signal Processing and Integrated Networks (SPIN). https://doi.org/10.1109/spin.2018.8474211

Simmons, R. (2016). The failure of the computer fraud and abuse act: Time to take a new approach to regulating computer crime. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2726662

Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. *2017 International Conference on Signal Processing and Communication (ICSPC)*. https://doi.org/10.1109/cspc.2017.8305855

Siniarski, B., Olariu, C., Perry, P., & Murphy, J. (2017). *Openflow based VoIP QoE monitoring in enterprise SDN*. https://doi.org/10.23919/inm.2017.7987354

Skerpac, V. (2019). Secure voice communications (Vol). *Information Security Management*, 191-210. https://doi.org/10.1201/9781351073547-15

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154-176. https://doi.org/10.1016/j.cose.2016.04.003

Song, H., Lynch, M. J., & Cochran, J. K. (2015). A macro-social exploratory analysis of the rate of interstate cyber-victimization. *American Journal of Criminal Justice: AJCJ, 41*(3), 583-601. https://doi.org10.1007/s12103-015-9308-4

Soni, A., Upadhyay, R., & Jain, A. (2017). Internet of things and wireless physical layer security: A survey. *Lecture Notes in Networks and Systems*, 115-123. https://doi.org/10.1007/978-981-10-3226-4_11

Souag, A., Mazo, R., Salinesi, C., & Comyn-Wattiau, I. (2015). Reusable knowledge in security requirements engineering: A systematic mapping study. *Requirements Engineering*, *21*(2), 251-283. https://doi.org10.1007/s00766-015-0220-8

Souppaya, M. P., & Scarfone, K. A. (2016). *Guide to enterprise telework, remote access, and bring your own device (BYOD) security.* https://doi.org/10.6028/nist.sp.800-46r2

Steinmetzer, D., Ahmad, S., Anagnostopoulos, N., Hollick, M., & Katzenbeisser, S. (2018). Authenticating the sector sweep to protect against beam-stealing attacks in IEEE 802.11ad networks. *Proceedings of the 2nd ACM Workshop on Millimeter-Wave Networks and Sensing Systems*. https://doi.org/10.1145/3264492.3264494

Stewart, H., Gapp, R., & Harwood, I. (2017). Exploring the alchemy of qualitative management research: Seeking trustworthiness, credibility, and rigor through crystallization. *The Qualitative Report*, *22*(1), 1-19. https://nsuworks.nova.edu/tqr/vol22/iss1/1/

Sumi, F. H., Dutta, L., & Sarker, F. (2019). A review on cyberattacks and their preventive measures. *International Journal of Cyber Research and Education*, *1*(2), 12-29. https://doi.org/10.4018/ijcre.2019070102

Suthar, D., & Rughani, P. H. (2020). A comprehensive study of VoIP security. *2020 2nd International Conference on Advances in Computing, Communication Control and Networking(ICACCCN)*. https://doi.org/10.1109/icacccn51052.2020.9362943

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, *68*(3). https://doi.org/10.4212/cjhp.v68i3.1456

Tait, A. R., & Voepel-Lewis, T. (2015). Digital multimedia: A new approach for informed consent? *JAMA*, *313*(5), 463. https://doi.org/10.1001/jama.2014.17122

Talla, V., Hessar, M., Kellogg, B., Najafi, A., Smith, J. R., & Gollakota, S. (2017). Lora backscatter. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *1*(3), 1-24. https://doi.org/10.1145/3130970

Tandel, H., & Rughani, P. H. (2018). Forensic analysis of asterisk-FreePBX-based VoIP server. *International Journal of Emerging Research in Management and Technology*, *6*(8), 166. https://doi.org/10.23956/ijermt.v6i8.133

Tchernykh, A., Cortés-Mendoza, J. M., Bychkov, I., Feoktistov, A., Didelot, L., Bouvry, P., Radchenko, G., & Borodulin, K. (2019). Configurable cost-quality optimization of cloud-based VoIP. *Journal of Parallel and Distributed Computing, 133*, 319-336. https://doi.org/10.1016/j.jpdc.2018.07.001

The National Commission for Protection of Human Subjects in Biomedical and Behavioral Research. (1979). *PsycEXTRA Dataset.* https://doi.org/10.1037/e301872003-001

Thiyagarajan, M., & Raveendra, C. (2017). Role of web service in internet of things. *2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*. https://doi.org/10.1109/icatcct.2017.8389146

Thomas, C. (2020). Introductory chapter: Computer security threats. *Computer Security Threats*. https://doi.org/10.5772/intechopen.93041

Thomas, D. R. (2017). Feedback from research participants: Are member checks useful in qualitative research? *Qualitative Research in Psychology*, *14*(1), 23-41. https://doi.org/10.1080/14780887.2016.1219435

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber-attacks. *Computers & Security*, *72*, 212-233. https://doi.org/10.1016/j.cose.2017.09.001

Tran, V. T., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology*, *80*, 88-96. https://doi.org/10.1016/j.jclinepi.2016.07.014

Tu, H., Doupe, A., Zhao, Z., & Ahn, G. (2016). SoK: Everyone hates robo calls: A survey of techniques against telephone spam. *2016 IEEE Symposium on Security and Privacy (SP)*. https://doi.org/10.1109/sp.2016.27

Tucker, K., Branson, J., Dilleen, M., Hollis, S., Loughlin, P., Nixon, M. J., & Williams, Z. (2016). Protecting patient privacy when sharing patient-level data from clinical trials. *BMC Medical Research Methodology*, *16*(1), 77. https://doi.org/10.1186/s12874-016-0169-4

Tunley, M., Button, M., Shepherd, D., & Blackbourn, D. (2017). Preventing occupational corruption: Utilizing situational crime prevention techniques and theory to enhance organizational resilience. *Security Journal*, *31*(1), 21-52. https://doi.org/10.1057/s41284-016-0087-5

Ukhaneva, O. (2015). *The changing nature of the telecommunications Industry: Impacts on demand and regulation* (Doctoral dissertation, Georgetown University).

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Education and Practice*, *6*(5). https://doi.org/10.5430/jnep.v6n5p100

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2015). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 169-188. https://doi.org/10.1177/1043986215621379

Valente, J., & Cardenas, A. A. (2017). Security & privacy in smart toys. *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy* (pp. 19-24). https://doi.org/10.1145/3139937.3139947

Van Manen, M. (2017). But is it phenomenology? *Qualitative Health Research*, *27*(6), 775-779. https://doi.org/10.1177/1049732317699570

Van Noorden, R. (2016). ArXiv preprint server plans multimillion-dollar overhaul. *Nature*, *534*(7609), 602-602. https://doi.org/10.1038/534602a

Varpio, L., Ajjawi, R., Monrouxe, L. V., O'brien, B. C., & Rees, C. E. (2016). Shedding the cobra effect: Problematising thematic emergence, triangulation, saturation, and member checking. *Medical Education*, *51*(1), 40-50. https://doi.org/10.1111/medu.13124

Vazire, S. (2018). Implications of the credibility revolution for productivity, creativity, and progress. *Perspectives on Psychological Science*, *13*(4), 411-417. https://doi.org/10.1177/1745691617751884

Velianitis, G. (2018). Comparison of VoIP and TETRA regarding security in a safety critical environment. *Journal of Computers*, 279-286. https://doi.org/10.17706/jcp.13.3.279-286

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

Wagdy, M., Babulak, E., & Al-Dabass, D. (2021). Network function virtualization over cloud-cloud computing as business continuity solution. *E-Service.* https://doi.org/10.5772/intechopen.97369

Westlake, C. P. (2017). *U.S. Patent No. 9,609,129*. *Washington, DC*: U.S. Patent and Trademark Office. https://www.uspto.gov

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J. (2017). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only, and the victimization-offending overlap. *Deviant Behavior*, *40*(1), 40-55. https://doi.org/10.1080/01639625.2017.1411030

Willgens, A. M., Cooper, R., Jadotte, D., Lilyea, B., Langtiw, C., & Obenchain-Leeson, A. (2016). How to enhance qualitative research appraisal: Development of the methodological congruence instrument*. The Qualitative Report, 21*(12), 2380-2395. *https://*doi.org/10.46743/2160-3715/2016.2361

Wolgemuth, J. R., Erdil-Moody, Z., Opsal, T., Cross, J. E., Kaanta, T., Dickmann, E. M., & Colomer, S. (2015). Participants' experiences of the qualitative interview: Considering the importance of research paradigms. *Qualitative Research*, *15*(3), 351-372. https://doi.org/10.1177/1468794114524222

Wu, Y. P., Thompson, D., Aroian, K. J., McQuaid, E. L., & Deatrick, J. A. (2016). Commentary: Writing and evaluating qualitative research reports. *Journal of Pediatric Psychology*, *41*(5), 493-505. https://doi.org/10.1093/jpepsy/jsw032

Yang, Z., Wang, W., Huang, Y., & Li, X. (2019). Privacy-preserving public auditing scheme for data confidentiality and accountability in cloud storage. *Chinese Journal of Electronics*, *28*(1), 179-187. https://doi.org/10.1049/cje.2018.02.017

Yao-Chung Chang, L. (2019). Criminological perspectives on cybercrime: Risk, routine activity, and cybercrime. *Research Handbook on Transnational Crime*, 327-343. https://doi.org/10.4337/9781784719449.00030

Yarygina, T., & Bagge, A. H. (2018). Overcoming security challenges in microservice architectures. *2018 IEEE Symposium on Service-Oriented System Engineering (SOSE)*. https://doi.org/10.1109/sose.2018.00011

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report*, *20*(2), 134-152. https://nsuworks.nova.edu/tqr/vol20/iss2/12

Yihunie, F., & Abdelfattah, E. (2018). Simulation and analysis of Quality of service (QoS) of voice over IP (VoIP) through local area networks. *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. https://doi.org10.1109/uemcon.2018.8796802

Zahid, H., Mahmood, T., Morshed, A., & Sellis, T. (2019). Big data analytics in telecommunications: Literature review and architecture recommendations. *IEEE/CAA Journal of Automatica Sinica*, 1-22. https://doi.org/10.1109/jas.2019.1911795

Zaslawski, Z. (2017). Not everyone is a target: An analysis of online identity crime victimization using routine activities theory (Doctoral Dissertation)

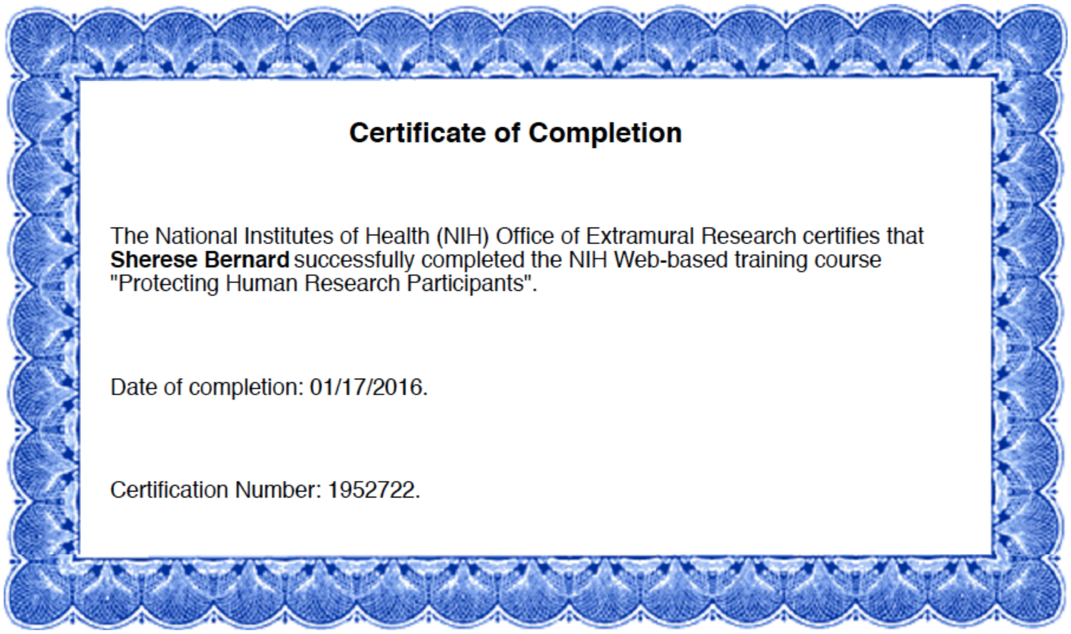
Zhang, L., Tang, S., & Zhu, S. (2016). An energy-efficient authenticated key agreement protocol for SIP-based green VoIP networks. *Journal of Network and Computer Applications*, *59*, 126-133. https://doi.org/10.1016/j.jnca.2015.06.022

Zhao, J., Bai, J., Zhang, Q., Yang, F., Li, Z., Zhang, X., Zhu, X., & Bai, R. (2018). The discussion about mechanism of data transmission in the OSI Model. https://doi.org/10.2991/tlicsc-18.2018.1

Zhao, P., Li, P., Ross, K., & Dennis, B. (2016). Methodological tool or methodology? Beyond instrumentality and efficiency with qualitative data analysis software. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research (Vol. 17, No. 2). ISSN 1438-5627.* http://www.qualitative-research.net/index.php/fqs/article/view/2597/3985

Zheng, Z., Webb, A., Reddy, A. L., & Bettati, R. (2018). IoTAegis: A scalable framework to secure the Internet of things. *2018 27th International Conference on Computer Communication and Networks (ICCCN).* https://doi.org/10.1109/icccn.2018.8487335

Appendix: Human Research Participants Certificate of Completion



Certificate of Completion

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

Date of completion: 01/17/2016.

Certification Number: 1952722.