2023

Strategies for Proper Security Practices in Small Financial Institutions

Adam Leffell
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Adam Leffell

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. Alan Dawson, Committee Chairperson, Information Technology Faculty
Dr. Bob Duhainy, Committee Member, Information Technology Faculty
Dr. Cynthia Phillips, University Reviewer, Information Technology Faculty

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

Walden University
2023

Abstract

Strategies for Proper Security Practices in Small Financial Institutions

by

Adam Leffell

MS, Western Governors University,2013

BS, Skyline College, 2012

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2023

Abstract

Financial institutions remain high targets for threat actors because of potentially lucrative financial gains from security breaches. Information technology (IT) security professionals in financial institutions are concerned about weak security strategies that could lead to security breaches. Grounded in the technology acceptance model (TAM), the purpose of this qualitative multiple case study was to explore strategies IT security professionals use to implement proper security practices to prevent security breaches. The participants were three IT security professionals from three different financial institutions that oversee the implementation of security policies and procedures. Data collection involved conducting semi-structured interviews and public documents. Through thematic analysis, four themes were identified: layered security, security auditing, technology adaptive, and vendor relationships. Recommendations are for IT security professionals to implement security in layers, review existing security controls and technology with current available market trends, and audit existing security controls to identify gaps with industry standards. The implications for positive social change include potential guidance for IT security professionals to able to strengthen an organizations security posture to better protect resources, intellectual property, and safeguard customer data from threat actors.

Strategies for Proper Security Practices in Small Financial Institutions

by

Adam Leffell

MS, Western Governors University, 2013

BS, Skyline College, 2012

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2023

Dedication

I would like to dedicate this study to my wife, Brea and my children, Cruz and Caia. This paper is proof that perseverance will pay off. A goal is always attainable, even when it feels so far away.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

Financial institutions are among some of the top industries that are faced with dealing with cyber-resiliency. The information and business function of financial institutions make them a viable target for threat actors. This requires the information technology (IT) security professionals employed by financial institutions to not only understand cyber security but have a firm grasp on how to deploy, monitor and react to cyber threats through policy and procedures. The issue that arises is that not all institutions are the same and the strategies employed to protect against data breaches may not be sufficient. Financial institutions must continuously monitor and innovate protected systems to ensure they do not become compromised (Cyriac & Sadath, 2019). In Tao et al. (2019), the financial industry must protect data stored, in transit, and usage of data through multiple business applications. This can become a challenging task for IT security professionals to implement proper strategies that are ever evolving due to the security landscape and their lack of knowledge and skill sets (Furnell, 2021). Therefore, in this study, my main objective was to explore strategies used by security professionals to implement proper security practices to prevent security breaches.

Problem Statement

The financial industry is completely reliant upon automated networking, information processing and telecommunication services (Varga et al., 2021). The dependency upon these services puts financial institutions at risk to cyber threats leading to data breaches. In 2018, the average cost of a data breach was $3.86 million, a 6.4

percent increase over the previous year (Ponemon Institute, 2018). The general IT problem is there is a lack of knowledge of strategies to use when implementing proper security practices for IT systems of small financial institutions. The specific IT problem is some IT security professionals lack strategies for implementation of proper security practices for small financial institutions.

Purpose Statement

The purpose of this qualitative case study was to explore the strategies used by IT security professionals for implementation of proper security practices for small financial institutions. The target population consisted of IT security professionals within small financial institutions in the southeastern United States. The findings from this study may benefit IT security professionals in establishing proper security practices when securing their financial institutions network, preventing data breaches. The implications for positive social change were safe and secure experience for members and employees of the financial institutions when conducting business and transactions.

Nature of the Study

The methodology that I chose for this research was a qualitative approach. As noted by Brantlinger et al. (2005), the qualitative approach is seen as a systematic approach that explores qualities, or essential natures of a phenomenon. My focus in this study was to explore strategies IT security professionals use to implement proper security practices for small financial institutions. I chose the qualitative approach over quantitative or mixed method designs. The quantitative method is used to focus on predictions, hypothesis testing, statistical analysis, and can include many different

instruments for data collection (Johnson & Onwuegbuzie, 2004). I did not choose the quantitative method for this study because I did not gather statistical data or hypothesis predictions. The mixed method approach includes both quantitative and qualitative approaches (Green et al., 1989). I did not focus on performing statistical analysis, hypothesis testing, during the exploration of the phenomenon. Therefore, I did not use a mixed-methods approach.

The design for this study was a multi-case study design. The case study design represents a research strategy to examine a particular phenomenon in real-life context (Yin, 1981). My goal for this study was to explore IT security professionals' strategies for implementing proper security practices to prevent security breaches. I explored different strategies used by IT security professionals to implement proper security practices to prevent data breaches.

There are other qualitative methodologies. One of these is the phenomenological approach, which is used to examine individual embodied experiences (Starks & Trinidad, 2007). Additionally, phenomenology researchers focus on understanding the individuals' lived experiences through their perception of experience (Starks & Trinidad, 2007). My goal for this study was to explore strategies used by IT security professionals to prevent security breaches but I did not focus on trying to understand the IT security professionals' perception toward security for preventing security breaches. Therefore, I did not choose the phenomenological approach.

The ethnographic approach is used to understand behaviors based on culture or social aspects (Goulding, 2005). I did not focus on cultural aspects, but on the strategies

used by IT security professionals to implement proper security practices to prevent security breaches. Therefore, I did not choose the ethnographic approach for this study. I chose the multi-case study design based on my overall goal for the study, which was to explore strategies used by IT security professionals to implement proper security practices within small financial institutions to prevent security breaches.

Research Question

What strategies do IT security professionals take to mitigate security vulnerabilities for their small financial institutions?

Interview/Survey Questions

1. What techniques do you use assess vulnerabilities?
2. What strategies are you applying to mitigate vulnerabilities?
3. What strategies are you using to prevent outside threats?
4. What strategies are you using to prevent internal threats?
5. How do you handle vendor remote management?
6. What strategies do apply to remote work?
7. What strategies do you implement for secure communication?
8. What strategies do you implement for Disaster recovery?
9. What level do you feel your current strategies protect you from threats?
10. What level do you engage end user feedback on existing security measures such as guidelines they must adhere to?
11. What strategies have you implemented that failed?
12. What challenges do you face with your current strategies?

13. What are some setbacks you have experienced after applying new security strategies?
14. What is some skill sets you think an IT security professional should posse?

Theoretical or Conceptual Framework

The theoretical model that I used for this study was the technology acceptance model (TAM). The TAM was formed by Fred Davis (Davis, 1985) based on principles of Fishbein and Ajzen's (1975) attitude paradigm from psychology (Davis, 1985). Fred Davis performed a study involving a field survey and a laboratory experiment where two business graphic systems with 40 MBA students as subjects, to evaluate the proposed model (Davis, 1985). Lee et al. (2011), explained that the concept of TAM is comprised of examining two components: *perceived usefulness* and *perceived ease* According to this model perceived usefulness is defined as the users' identification of how useful the product or service will benefit them in their life or job role and perceived ease is the degree of effort the users must put forth in using a service (Lee et al., 2011). In this study, the TAM model was essential in defining strategies used and adopted for security, based on user acceptance, but also usefulness. I applied the TAM by exploring the strategies used by IT security professionals to implement proper security practices to prevent security breaches. By exploring these security practices through the TAM model, I examined the strategies that IT security professionals choose when implementing proper security. I used the TAM model for this study to understand strategies used for proper security practices within small financial institutions to prevent security breaches.

Definition of Terms

Security Procedures: A set sequence of necessary activities that perform a security task (Fay & Patterson, 2018).

Security Professional: one who is technically sound to assemble layers of security to protect an organization by implementing policies and procedures (Andress, 2014).

Assumptions, Limitations, and Delimitations

Assumptions

Almasri and McDonald (2021) stated assumptions are a combination of the researchers' values, beliefs, knowledge of the topic researched, and inevitably shape the research process. My first assumption in this study was that the participants would contribute honest and accurate responses to my questions resulting in quality data. My second assumption was participants would be able to provide documentation of internal policies to contribute to my study, again resulting in quality data.

Limitations

Theofanidis and Fountouki (2018) stated that limitations can be potential weakness of the study that are out of researchers control and may affect the study. A limitation of this study was the small geographic location of the study being in central region of Virginia. Secondly the reliance upon small financial institutions to reveal adequate documentation of their internal policies may narrow the findings, leaving potential themes undiscovered.

Delimitations

Theofanidis and Fountouki (2018) defined limitations as boundaries set by the researcher within the study. A delimitation of my study was the geographical location of my study within the central region of Virginia. Small financial institutions outside of central region of Virginia may provide additional resources for my study but would be placed outside of the scope and therefore not participating in the study. Lastly the population sample size remained small due to the scope of the geographical location being narrowed to just the central region of Virginia.

Significance of the Study

Vulnerabilities in IT systems are not new and are on the rise. Between 2010 and 2015 about 80,000 new vulnerabilities were registered within the CVE database (Jurn et al., 2018). While advancement in IT security and research has improved within the past 20 years, security professionals still lack proper vulnerability management (Jacobs et al., 2020). Although research surrounding this topic is available, additional research could provide further understanding surrounding best practices for proper security practices. Therefore, this study could be beneficial to IT security professionals when dealing with strategies to implement proper security practices to prevent security breaches.

Contribution to Information Technology Practice

When IT security professionals fail to properly implement proper security and harden information systems, they are exposing themselves to possible attacks. Security breaches can become a costly loss for a business with the average cost of $21,155 per day (Jeong et al., 2019). While a business might face financial loss, they may also lose loyal

customers due to a breach. This study could include insight into managing security vulnerabilities and may be beneficial to other IT security professionals looking for strategies to improve their security baselines.

Implications for Social Change

The opportunity for social change is beneficial for individual users and businesses. Kay et al. (2021) stated that most businesses and individuals have some sort of interactions with financial institutions and their personal data is on file with the institution. By providing insight to strengthen the overall security practices, institutions can better protect themselves to prevent customers' personal data from falling into the wrong hands. This benefits individuals and businesses interacting with financial institutions as they know steps are being taken to protect their privacy while providing financial services.

A Review of the Professional and Academic Literature

The literature review is a foundational component of all academic research, according to Snyder (2019), an accurate literature review is constructed by building research on and relating to existing knowledge. Furthermore, an author can highlight areas that require further research by synthesizing current literature and exposing areas of research that are disparate and interdisciplinary (Snyder, 2019).

I gathered information for this literature review from various sources within Google Scholar, SAGE, Elsevier, ProQuest, Walden's University Library, and a few other scholarly databases. The content within the databases searches contained conference proceedings, dissertations, journals, and peer-reviewed articles. I narrowed

my search results by using key words which included: *proper security practices, financial security guidelines, implementing best security practices, InfoSec, vulnerability management, patch management, remote work, covid-19 remote work, penetration testing, multifactor authentication, IT governance, security awareness training, IT security practices, disaster recovery, vendor management, vendor control,* and *network security.* I synthesized information from 78 resources for the literature review. Out of those, 47 publications (60%) were peer-reviewed and 44 (57%) were published between 2018 and 2023, 57 were discovered through Walden library (73%) and 21 through Google Scholar (27%). I established a scholarly foundation for the study while providing a critical analysis of the body of knowledge related to the central research question for this study: What strategies do IT security professionals take to mitigate security vulnerabilities for their small financial institutions?

Conceptual Framework

I chose the TAM model as the primary theory for this study based on the review of available literature related to the research question on the strategies used by IT security managers in mitigating security breaches within small financial institutions. The TAM was formed by Fred Davis (Davis, 1985) based on principles of Fishbein and Ajzen's (1975) attitude paradigm from psychology (Davis, 1985). Davis (1985) stated that a system's features and capabilities directly influence a users' motivation for using the system. The TAM was used to address the process for understanding acceptance of technology and the uses by consumers of that technology (Sinha & Mukherjee, 2016). While many studies have attempted to address the consumer adoption issue, The TAM

model has proven, through numerous studies, to consistently explain usage intention and behavior action. While there can be many variables that play into the user acceptance of the TAM model, the main two components are perceived usefulness and perceived ease of use.

The perceived usefulness is best described as the extent a person will or will not use a system based on how much the user believes it will help them to perform their job better (Sinha & Mukherjee, 2016). The perceived ease of use is based on how easy an individual believes a system is to use. There is a direct correlation that perceived ease of use can directly influence perceived usefulness, in that if a system is useful, but too difficult to use, the adaptation of the system will still fail. Dash et al. (2011) stated that the TAM has been proven to a be a powerful framework in predicting user acceptance of new technologies with 40% evidenced effectively in determining system use. In the following section I will further discuss the TAM model and its relation to IT specifically within the financial industry.

Technology Acceptance Model

The TAM was introduced by Fred Davis (Davis, 1985). In Davis's doctoral research thesis, the conceptual framework for TAM is used to explain that the system features, and its capabilities would have a direct effect on the users' intention to use the system. These beliefs stem from two existing theories, the theory of reasoned action (TRA) and theory of planned behavior (TPB). The TRA is by researchers M. Fishbein and I. Ajzen, where Fishbein and Ajzen suggested that a users' attitude affect their behavior (Ajzen & Fishbein, 1977). The TPB is by I. Ajzen and T. Madden, where the

theory was used to understand perceived control over behavioral achievements to determine intention and behavior (Ajzen & Madden, 1986). While the TRA and TPB have previously been used to identify technology acceptance and consumer behavior, the TAM was introduced to build upon the gaps of TRA and TPB towards individuals' intentions to use technology (Hu et al., 2019). Sinha and Mukherjee (2016) stated that Fred Davis tried to explain that the absence of user acceptance is a barrier to the success of a new information system. Since the TAM is derived from both the TRA and the TPB, when used, the TAM can show the relationship between system design, the perceived ease of use and the perceived usefulness (Sinha & Mukherjee, 2016). This shows that the TAM model can be used to predict the users' intentions to a system based on five variables, perceived ease of use (PEOU), perceived usefulness (PU), behavior intention (BI), attitude and external variables.

Perceived Ease of Use

PEOU illustrates the users' perception of the amount of effort that will be required to use a system. If the user perceives that a system requires too much effort, then the system is less likely to be accepted by the user (Davis, 1989). This perception is influenced by two factors: self-efficacy and instrumentality. Self-efficacy explained by researcher Bandura in 1982 and stated that the easier a system is to use, then the higher a users' self-efficacy will become. In instrumentality, the users will be able to spend less effort if a system is easier, making the completion of tasks more efficient. Thus, instrumentality may affect overall job performance resulting in the users' perception of a system to be a more positive accepting manner.

Perceived Usefulness

PU depicts a user's belief regarding how useful a system may improve their work efficiency (Hu et al., 2019). The higher the PU, the more positive the user believes that there is a benefit in using a system. Davis (1985) stated that a system with a high PU will be perceived, from a user standpoint, a positive use-performance relationship. Thus, making PU a direct factor on the determination PEOU.

Attitude

Attitude is a perception toward an object, idea, or person. Ajzen and Fishbein (1977) stated that attitude is expressed as the user's evaluation of the question at hand. This is typically defined as either positive or negative and that a positive attitude in relation to a new technology can predict a user's intention to accept the technology. Davis (1989) stated that attitude within the TAM is different than that related toward behavior. Attitude toward PEOU and PU is merely based on users' value toward performance and effort, not objective reality.

Behavior Intention

Behavior criteria according to Ajzen and Fishbein is an observed action performed and recorded (Ajzen & Fishbein, 1980). Behavior may have different outcomes when compared with attitudes. A user's attitude may predict the consistency in which a behavior occurs (Ajzen & Fishbein, 1977). The behavior can be interpreted as the intention to use a technology. If the user has a positive attitude toward a technology the BI may become more consistent oppose to someone who projects a negative intention on the same technology.

Subject Norm

Subject norm (SN) is derived from the TRA and was not originally included in the TAM model but as stated in Abbas (2016) later added during the emergence of TAM2. SN is the individual's perception of what people think who are important to the individual when faced with a behavior situation (Abbas, 2016). Like attitude, the SN may alter the behavioral intention to use, if the individual believes, there is a negative or positive influence from ones' peers (Dash et al., 2011).

Information Security and TAM

Each variable is an important role in the prediction of the TAM model to understand whether a user accepts or rejects a technology (Dash et al., 2011). Security policies and practices may be designed to prevent security breaches, but if policies and guidelines make a system difficult to use, end users may try to find alternate ways around these policies. Pham et al., (2019) stated that a users' inability to follow security policies leads to more than 40% of security breaches. This becomes an issue for IT security professionals as manipulation of a system or policy may expose new vulnerabilities and exploits resulting in a security breach. Security practices and hardening of systems, must be accomplished in a way that will be received and accepted by users to ensure they're used as intended and without manipulation. This requires that employees have a positive emotion toward information security requirements to sustain proper security practices (Pham et al., 2019).

The role of an IT security professional is to implement and safeguard over information systems assets. This includes identifying potential security vulnerabilities

that apply to the system and in what way it might affect the system based on how the system is intended to be used. The IT security professional must address how to mitigate these identified vulnerabilities to prevent exploitation of the system from compromising the integrity of a system. This can include creating and applying a strategic security plan to prevent exploitation from the known vulnerabilities and then altering as new vulnerabilities are discovered (Bayuk & Silverstein, 2007).

Each vulnerability that is discovered on a system is categorized as a risk and must either be mitigated or accepted by the organization. Because risks can never be eliminated completely, it is important to establish a balance between risk and usability of a system. Applying too much of either may results in the system being unusable or compromised. By using the TAM as an influential framework, IT security professionals can create a balance between security and usability of a system to increase user intention of a system (Dash et al., 2011).

Security framework models construct a baseline for the security policies and procedures that are put in place. While there are many different types of frameworks available, all frameworks conform around three core ideas: Confidentiality, integrity, availability. These three core components comprise what is called the CIA Triad. Aminzade (2018) stated the CIA is used as a basis for establishing IT risk assessments while balancing between the CIA. Again, focusing too much on one may result in the other becoming a weak point resulting in an exploitation. Each component for the CIA is discussed below.

Mishra et al. (2018), briefly described confidentiality as protecting data and information from unauthorized access. This safeguarding prevents unauthorized users from being able to see, access, or even alter information. Only authorized users should have the ability to interact with the system.

According to Kumar et al. (2015) integrity is sustained by being able to verify that data has not been altered, lost, or compromised in any way; maliciously or accidentally. Furthermore, integrity is assurance to a recipient during transmission of data that the data has not been altered or changed by anyone other than the originating source. Integrity does not provide confidentiality; integrity is designed only to provide validation that the data has not been altered by anyone else other than the originating source.

Availability consists of making sure data resources are available and that authorized users have access to data resources on a needed basis. This ensures data and systems remain online and available for interaction and use. A threat to availability would consist of making data or a system inaccessible to a user (Kumar et al., 2015).

The CIA triad is useful to IT security professionals when creating mitigation strategies. By considering each portion of the CIA, the IT security professional can limit the possibility of exposing a new weak point of a system when implementing a mitigation strategy. System weak points and vulnerabilities are often found when an IT security professional conducts a threat analysis. In a threat analysis systems asset are evaluated and ranked according to associated risk (Fockel et al., 2018). Once the threats have been identified and evaluated a system design can be created. This can involve designing and implementing policies or procedures. While creating policies and access controls is

constantly evolving, the gap in secure environments come from compliant and noncompliant behaviors (Belanger et al., 2017).

Compliant and noncompliant behavior stems from a user's attitude toward a security policy, when the security policy is forced, this can cause a user to have a negative attitude toward compliance with a security policy. When users nonconform to a security policy it can cause new vulnerabilities to arise that the IT security professional may be unaware of. According to researchers Belanger et al., (2017) an organization should encourage early conformance for proactive users toward a password policy prior to being forced to use comply with a policy. Belanger et al. (2017) stated that users who conform to security policies early are less likely to cause unwanted security behaviors later. Using the TAM model to gauge users' attitude and behavior towards a security policy may predict the adoption rate of the security policy, even if the policy is to be enforced.

Incorporating the CIA triad with the TAM model is beneficial in the success of system adoption, by using the CIA triad and the TAM, the IT security professional can focus on determining the perceived risk a user might perceive. This is seen in other studies where researchers have incorporated variables into the TAM model. Researchers Kesharwani and Bisht combined TAM with the variable perceived risk to evaluate the adoption rate challenges IT security professionals faced when offering safe and secure virtual environments with internet banking (Kesharwani & Bisht, 2012).

Because the customer experience will differ in an open environment than it would in a traditional transaction experience, their perceived risk will be higher. Couple the

perceived risk with the notation that online services are susceptible to online-attacks, such as phishing and malware, then the users' perception of online banking my negatively impact their behavior toward internet-banking. Hu et al. (2019) extended the TAM model with contributing factors of brand image, government support, and user innovativeness. Being the trust a user constructs toward a system is shaped by each factor. Trust and brand image correlate together as a user builds trust based on brand image. A brand image is shaped by the guarantee of products and services the business offers (Hu et al., 2019).

In addition, combining the TAM model variables such as social influence affect the brand image. When the brand image is positive, trust is increased, reducing perceived risk, increasing positive attitude, and increasing positive BI. Therefore, trust is a significant factor in reducing perceived risk regarding the financial sector (Hu et al., 2019).

The financial sector is a dynamic multi-channel driven industry, it is perceivable to see perceived risk and usability forms of different channels (Munoz-Leiva et al., 2017). To reduce perceived risk, there must be proper security controls in place, this requires proper implementation of security policies and procedures by the IT security professional. The security policies and procedures come from the IT security professional's perspective on the severity of a perceived risk and their ability to handle the potential threat. Thus, proper security practices may depend on how the IT security professional is equipped to identify and handle an IT security threat (Hooper & Blunt, 2020). Several studies have been conducted that focus on employees' intentions to

violate information security policies regarding behavioral intentions. Mostly, these studies look at non-IT staff and their behavior toward information security. According to Hooper and Blunt (2020), the exploration of IT staff behavior toward information security remains unexplored.

Analysis of Supporting Theories

The objective of this study was to explore the strategies used by IT security professionals to implement proper security practices within small financial institutions. The TAM is a theoretical framework widely used and validated as a powerful framework to predict user acceptance of a new technology (Dash et al., 2011). The TAM is frequently used in Information Systems and has proven to predict 40% effectiveness toward system acceptance (Harryanto et al., 2018). Using the TAM, IT security professionals can critique their security practices to ensure proper security is in place while alleviating non-compliance from users. The TAM relates to other theories, such as the planned behavior theory (TPB), the theory of reasoned action (TRA), and the protection motivation theory (PMT).

Theory of Planned Behavior

The TPB is a framework that is derived from investigating measures of attitude and actions that predict an individuals' behavior (Ajzen & Fishbein, 1977). According to Hong and Funell (2019), the more positive a user's attitude is, the bigger the behavioral intention will be. When new technology becomes available, one of the factors that may depend on the adoption of the technology is users' behavior (Sungur-Gul & Ates, 2021). The TPB is used to explain individual behavior toward security compliance. According

to Tam, et al. (2022), in an attempt at understanding influences that make an employee follow security policies. A new user, while understanding it is a security requirement to lock their station when away from their desk, may abandon the security requirement because their new fellow coworkers don't follow the required security practice. In attempt to fit in, the new employee also objects the security practice and abandons locking their station in attempt to fit in. In the competitive market of the financial industry, it is important to understand employees' perception of technology tools available to satisfy customer demands (Yoo & Jung, 2019).

Theory of Reasoned Action

The TRA is a general model and was one of the first models use to study the acceptance of technology (Arenas-Gaitan et al., 2015). Introduced by Ajzen and Fishbein, (1980) TRA presents behavioral intentions combined with attitude and social norms factor the person specific behavior. The TAM was derived from the TRA and added in PU and PEOU (Ahmad, 2018). In a competitive environment user attitude and behavior is an important factor in determining actual system use. An individual's desire to comply with security policies is significantly determined by others' perceptions on how the individual should cooperate (Hooper & Blunt, 2020). Organizational culture can positively influence user behavior as well, Cuganesan, et al. (2018) stated senior management positive compliance with security controls can create a trickle-down effect on individual behavior and attitude of security adherence.

Protection Motivation Theory

The PMT is a framework originally developed to understand how fear shapes a person attitude and behavior (Prentice-Dunn & Rogers, 1986). The PMT consists of two main factors, Threat appraisal and coping appraisal that influence certain behavior. PMT combined with the self-efficacy theory presented in Maddux and Rogers (1983) proposed the importance of self-efficacy and the impact it has on BI. A person's ability to evaluate the severity of a technology may impact their intentions if they feel it as a threat. The use of security awareness training can improve an employee's ability to perceive and evaluate a potential threat (Silic & Lowry, 2020). Using PMT as a tactic for security training of employees, exposes the threats of information systems and can shape an employee's behavior toward following security guidelines (Mwagwabi et al., 2018). Hooper and Blunt (2020) stated the PMT is used to understand BI for IT employees with regards to information security. Intention shapes the user's behavior, this is prevalent in not just PMT, but also in TAM.

Contrasting Theories

Implementing IT security best practices comes in many forms. Each IT security professional may have a different take on how they approach some of the same risks. The TAM model created by Davis (1989), is designed to focus on the user attitudes surrounding PU and the PEOU. This may factor how the IT security professional focuses their attention to protecting their network and implementing proper security practices. In the following section I discuss the Task technology fit theory, Expectation Confirmation Model and how they differentiate from the TAM.

Task Technology Fit Theory

A different approach may be done by utilizing the Task Technology Fit Theory (TTF). The TTF is different from the TAM by focusing on the user task at hand and the available functionality of the IT (Dishaw & Strong, 1999). When the TAM is used for adapting a technology the focus is on the user's perception for how well the technology will achieve their task. This takes an approach of planning out a technology that the user will accept and use to benefit their job performance. This can be seen as a voluntary acceptance with the technology.

The TFF is more task focused on making sure the technology available is beneficial at completing tasks and the TFF is less focused on users voluntarily accepting the technology. The TFF is designed on making sure the available technology will be best suited for completing the tasks at hand (Dishaw & Strong, 1999). According to Howard and Rose (2018), the TTF theory proposes that there is a positive impact when a technology is matched with a specific task. Often when applying proper security practices, IT security professionals use the best tools available for ensuring mitigation tactics are applied. This may not always have users' best interest in mind but may provide a secure system for completing tasks.

TTF can often be an afterthought to user acceptance where the TAM model is seen as more of a pre-planned technology with user acceptance in mind (Dishaw & Strong, 1999). When it comes to the TTF theory, the performance outcome is the main component. The user reactions that are perceived from TTF are impacted by the technologies ability to handle and complete a task with best performance. Thus, the user

is expected to understand the performance outcomes that a technology is capable of and should make the interaction with the technology enjoyable.

While the TAM predicts user acceptance based on attitude and behavior toward the technology, it does not really consider the performance, processing, or transmission capabilities that a technology may consist of; while the TTF takes these characteristics into account (Dishaw & Strong, 1999). The TTF does not factor in user acceptance and willingness to use a technology, but on performance of a technology. Therefore, I did not choose this theory for my study. The focus of this study was to explore strategies used by IT security professionals to employ proper security practices to mitigate data breaches. This required that systems and practices put in place by IT security professionals were met with positive acceptance of users and not neglected or manipulated in such a manner to cause security breaches.

Expectation Confirmation Model

The Expectation confirmation model (ECM), unlike the TAM, is used to investigate the success of a technology post initial use. According to Bhattacherjee (2001), the ECM is used to understand the continuance of a technology. The initial acceptance of a technology is important, but the overall success of a technology is dependent on the user's participation of continued use after their initial acceptance of a technology. Laio et al. (2009) stated there are three main differences between ECM and TAM. First, in TAM the focus is on behavior for initial use, while ECM is used to explain retention and user loyalty toward are technology. Second, user behavior toward a system will determine the user's attitude. In ECM the attitude and behavior are affected

by satisfaction from the outcomes with the technology. Lastly, the TAM elements used for initial adoption are based around PEOU and PU.

The ECM being a model for post activity focuses post consumption expectations. The ECM is used to understand user expectations versus perceived performance in determining the post expectation that may affect the users' loyalty to a system. While the TAM is an important factor to IT security professionals when thinking of proper security practices, the ECM may determine longevity of systems retention. Since technology is constantly evolving and new risks are exposed daily, an IT security professional must understand system adoption and longevity for protecting assets and maintaining a sound security posture.

This study was to explore strategies used by IT security professional for proper security practices. The ECM is based on perceived performance and expectations resulting in continuation to a technology. This often comes after the initial evaluation of PEOU and PU (Park, 2020). Therefore, I chose not to use the ECM for this study.

In reviewing both the TTF and ECM compared to the TAM there are different lenses that can be used to identify system acceptance. In the following sections I discussed some of the themes and technology used from the literature that IT security professionals may use to mitigate vulnerabilities when implementing proper security practices.

Themes from Literature

In this section I introduced themes and technologies used for mitigating vulnerabilities when constructing strategies for best security practice. A small financial

institution is held to a high fiduciary responsibility and there are many themes and technologies that can be incorporated to mitigate vulnerabilities. The following themes are outlined for their use and how an IT security professional may use them in their security strategies for proper security practices.

Security Appliances

Security appliances are seen as logical and physical appliances that can segregate a network both externally and internally. Some of the most common types of security appliances are firewalls, switches, routers, intrusion prevention and intrusion detection systems. Firewalls including demilitarized zones are a widely used security appliance and techniques throughout organizations.

Firewalls and DMZ

Firewalls and Demilitarized zones are often thought of as the first line of defense when it comes to external versus internal networks for an organization. The demilitarized zone (DMZ) is typically the portion of an organization's network that is accessible from the internet. A DMZ may be referred to as perimeter network security since its main function is to protect internal networks from external networks (Benqdara et al., 2018). Establishing a properly configured DMZ provides an enhanced layer of security by isolating services that must be available external from fully reaching an organization internal resource. In Ndichu et al. (2020), a DMZ provides security by isolating external traffic to a specific area of the business' network. This prevents malicious traffic from reaching the internal network but can leave the appliance that is hosted in the DMZ vulnerable. The main goal in using a DMZ is to provide services such as web hosting or

email externally without exposing internal network resources. Services that are hosted in a DMZ are often placed by behind a firewall to limit their internet exposure.

Firewalls are designed to limit and control the interaction between different networks (Jingyao et al., 2019). A firewall will either pass or block traffic based on the set of rules created by the IT security professional when receiving or sending traffic. Thus, firewalls can prevent malicious traffic from enter or exiting a network (Alvarez et al., 2021). Firewalls come in either hardware or software form, hardware firewalls are physical appliances that reside on an organizations network and process traffic from different networks. A software firewall may reside on an end point devices and process traffic to and from that end point device only. Hardware firewalls may operate under three main functions, packet filtering, application proxy, and stateful inspection (Jingyao et al., 2019).

In packet filtering, packets are inspected by the firewall. The packet will either be passed or dropped based on the source, destination, protocol, and port of the packet. Application proxy works as a gateway for internal devices. The firewall will take packets and then process them to hide the identity making them seem as though the firewall itself is the one sending and receiving the information (Jingyao et al., 2019). Lastly, stateful inspection is an enhanced version of packet filtering and maintains a table of open existing connections. Each packet is reviewed and while the connection is established between the source and destination, the firewall inspects the packets and monitors for malicious activity. (Jingyao et al., 2019).

Firewalls and DMZ are used together to enhance the overall security of appliances operating in a DMZ by limiting access to the DMZ based on the organization's services being offered. While firewalls and DMZ are available to enhance overall security, they are not a one size fits all operation. Firewalls and DMZ still contain weak points for malicious actors to get inside a network (Klein, 2021). Firewalls do not inspect and monitor encrypted traffic. Encryption is an entry way for malicious activity if the firewall does not have the ability to view the traffic. According to Klein (2021), 70% of malicious attacks are conducted with encrypted traffic. This requires the IT security professional to use different strategies along with DMZ and firewalls. When implementing firewalls and DMZ careful planning must be considered to ensure human error does not leave open vulnerabilities exposed for potential attackers (Alvarez, et al., 2021).

Intrusion Detection and Prevention Systems

Intrusion prevention systems (IPS) and intrusion Detection systems (IDS) are considered a second line security defense and are typically placed behind firewalls and reside either internal or within a DMZ (Wang, 2017). Both IPS and IDS are used in addition to other security appliances to inspect and monitor traffic for malicious activity. Unlike firewalls that are preventing external traffic from reaching internal traffic, IPS and IDS monitor all traffic that flows within an organization (Jaber et al., 2021). Both IDS and IPS operate behind firewalls which is why they are often referred to as second line of defense security appliances. Once traffic has made it beyond a firewall, the traffic is

allowed to continue to traverse along its destined route and will be monitored by either an IDS or and IPS.

An IDS is typically referred to as passive detective. The IDS monitors traffic at either network or host level and depending on triggers and sensor set by an administrator, will be activated once a packet meets the sensor threshold. When a sensor is activated, the IDS will alert an IT personnel that an intrusion is detected. This requires intervention by IT staff to investigate and determine if further action is required (Martinez & Vogel-Heuser, 2018). In an IDS nothing more is done, just a notification is triggered, and the traffic is allowed to continue. In an IPS, all the same functionality is there as an IDS, but a IPS can take corrective action on the packets, such as: dropping the packet, terminating the session, or even quarantining the information until further investigation can be done (Baykara & Das, 2018).

Both IDS and IPS operate under two main functions, Signature based detection and Anomaly-based detection. In signature-based detection, each packet that passes through an IDS/IPS is compared to signature that will meet a specific threshold. This can be pattern, connection, or string based and relies on relies on updated signatures to be applied to the appliance continuously (Wang, 2017). In anomaly-based detection is used to monitor patterns and behavior. This type of detection does require more time to create a baseline and monitors for abnormal activity taking place on a network (Wang, 2017). Each appliance is useful in detecting malicious or unwarranted traffic and provide benefits to and IT security professional best practices.

HoneyPots

The implementation for IDS and IPS can alert and possibly stop intrusion on a network but both intrusion systems monitor traffic and look for patterns or anomalies. When IT professionals want to see what a potential threat actor is doing in hopes to mitigate vulnerabilities, a honeypot might be beneficial. A honeypot is designed to imitate a legitimate system or possibly a whole network that doesn't truly house real data. When a honeypot is stationed on a network, the main goal is to deter a potential threat actor into attempting to attacking the honeypot in hopes of identifying possible flaws or holes within a network, so that the production network can then be patched to prevent an attack. Honeypots are beneficial in that they can reduce false positives and potential identify zero-day exploits that may be vulnerable in a production system (Baykara & Das, 2018). Furthermore, Baykara and Das (2018) stated that honeypots are not used for detecting intrusions, but more for understanding and learning how an attacker is enumerating the network based on specific criteria available. This provides a logged analysis for what a potential attacker may be able to gain or infiltrate without having to worry about the loss of real data.

Remote Management / Vendor Management

Information systems come in wide varieties and depending on the organization mission, they are typically vendor specific programs that are used to meet every business need. This opens the door to third party vendors and the ability for employees to access required resources when outside of the business. According to Cleary and Mclarney (2019), a vendor is referenced as a third party providing a product or a service. When a

business introduces a third-party product, vendor, or application into their organization, vendor management of that system should be established (Cleary & Mclarney, 2019).

A vendor management system is something most business must deal with, unless all programs and services are built in-house, then a vendor/third party is typically involved. Granting a vendor access to an organizational resource externally opens the business up to potential more vulnerabilities, as the control of security shifts from not just the business but to the vendor that has remote capabilities. However, controlling remote access is nothing new, and security measures are available to lower the risk of remote access. One of the main and effective ways to accomplish this task is with virtual private networks (VPNS).

VPN networks create an encrypted channel over a public network to ensure the communication of data is kept confidential (Kaur & Sharma, 2020). VPNS are cheap and easy to implement but do come with some security concerns. According to Ndichu et al. (2020), VPNS pose a risk to an organization as VPNs evade firewalls and IDS by encrypting all the traffic traversed between the connected devices. Still when it comes to remote workers and vendor management VPNS are an easy option and do provide encrypted communication between both parties.

Mobile Device Management

Mobile device management (MDM) consist of creating policies and guidelines surrounding mobile devices such as, smart phones and tablets. The advancement of mobile devices has allowed them to move from just personal gadgets and into business (Abu Othman et al., 2021). This adoption has expanded mostly due to the increase in

computing power and availability for connectivity almost anywhere (Batool & Masood, 2020). When looking at mobile device management there are two types of channels for MDM, company issued devices, and bring your own device (BYOD).

Company issued devices are provided, controlled, and owned by the organization. In company issued devices, there may be limitations on the functionality that the device has, and the device may be restricted to only serve a singular purpose. In BYOD the devices are owned by the individual and are allowed to access company resources. The BYOD has become a popular trend over the past few years for many reasons. Batool and Masood (2020) stated some of the reasons pointed out are initial reduced expenses on an organization, increased flexibility of work, and improved productivity due to ease of use for employees. Some organizations also see that preventing employees from bringing in their own device is just too hard to prevent (Abu Othman et al., 2021).

While there are many benefits for mobile devices, there are a lot of vulnerabilities and security concerns that must be considered. Allowing access to corporate networks opens an organization up to new threats and potential data losses, which requires management policies and controls to be put in place. The purpose of MDM is to enhance the security and guidelines of acceptable use, for not only company issued, by employee-owned devices as well (Batool & Masood, 2020). Things that are often considered when implementing MDM policies are monitoring, securing, encrypting, location tracking, malware detection, and remote wiping of devices.

Vulnerability Scanning/Identification

Identifying and handling vulnerabilities within an organization is a daunting task for IT security professionals. Jacobs et al. (2020) stated vulnerability management is a critical challenge that many businesses struggle with. There will always be more vulnerabilities than fixes due to software flaws developed by humans, most possible containing zero-day exploits. A business must face the dilemma of identifying the most critical exposures and then prioritizing those risks on which to mitigate first. When it comes to vulnerability scanning and identification, the biggest factor for organization is typically time.

The time that a vulnerability is identified, to the time the vulnerability is mitigated greatly depends on the patching strategy employed by the organization. According to Furnell (2016), patching is viewed as important, but still not an obligation to prioritize. Many businesses see the need for mitigation critical vulnerabilities but hold off due to consequences that failed patches might cause once deployed. This is from a lack of confidence in the ability of the mitigation not breaking other systems (Furnell, 2016). While there are many tools available for vulnerability scanning and identification, systems ultimately go unpatched due to insufficient strategies on how to prioritize patching (Jacobs et al., 2020).

Penetration Testing

Using vulnerability scanning to identify risks is used by IT security professionals to get a visual understanding of the vulnerabilities within an organizations network. Penetration testing is exploiting those vulnerabilities to test their risk factor (Johari et al.,

2020). Penetration testing is important to organization in producing a well-designed IT security strategy since penetration testing will expose and attack the vulnerabilities an organization has. This provides insight on what a threat actor may be able to accomplish if a vulnerability is ignored. Since companies want to protect their data, performing penetration testing is beneficial when deciding which vulnerabilities need to be prioritized. The issue many businesses face is the lack of knowledge or experience with cybersecurity professionals able to perform successful penetration testing. While the cybersecurity industry is demanding, many businesses are facing a shortage of pen testers, with 65% not having cyber security professionals on staff, and those that do, 35% have staff that is under trained (Chowdhary et al., 2020).

Encryption

Encryption or quite frequently referred to as cryptography and provides a secure means for protecting information. Encryption is used to encode data thus making the data secure when it is either being stored or transmitted between devices. This allows organization to conduct business electronically without the worry of the information being seen by unauthorized intentions (Goshwe, 2013). There are many forms of encryption however, I mainly focused on ones that provide protection for authentication and data protection in this study.

Encrypting data at rest comes in many forms and can be interpreted as any number of bits that reside on a physical medium. According to Matloob and Siddiqui (2017), it is expected that data is to double about every 2-3 years. This causes concern as organization continue to retain this data, Matloob and Siddiqui (2017) stated 44% of data

loss occurs due to physical media being lost or stolen. One of the most efficient ways to secure data when it is not being used is by encrypting the data at rest. This means using a cryptography algorithm to hide the true contents of the data until the data is to be used. For a business to understand what preventative measures they need to take to secure their data, the business needs to answer questions regarding the data they plan to retain. Matloob and Siddiqui (2017) stated the risk questions may include: Who has access to our data; Where, when, and how is our data being accessed; What type of data are we storing; What means is our data being accessed through? These questions can identify such risks as data manipulation, unauthorized access, and even insider attacks on organizations data (Abdulghani et al., 2019). As data retention continues to grow it is likely that data will span across multiple physical means to provide sufficient space, this requires proper protection to reduce the likelihood that personal identifiable information doesn't fall into unauthorized hands. Performing proper risk assessments on stored data and planning for proper storage, a business can reduce that risk and retain that data for as long as they need (Matloob & Siddiqui, 2017).

The internet protocol security standard or referenced as IPSEC provides a secure communication channel for transmitting data from one end point to another. The IPSEC protocol is certified open-source framework that provides creditability and integrity between the connecting parties (Mahmmod et al., 2020). The IPSEC technique is comprised of two main protocols, the authentication header (AH), and the encapsulating security payload (ESP). The AH provides unencrypted signature of each packet, while the ESP applies encrypting with signatures.

Each of the protocols operate independently, but also simultaneously (Mahmmod et al., 2020). The AH consists of authentication and integrity checks of the data that is being passed. One technique of this is though using message digest to prove the data has not been altered in transit. The ESP provide encryption, authentication, and integrity, The encryption takes place within the IP layer of the OSI model using various symmetric encryption protocols. The authentication procedures operate like the authentication header with message digest. This prevents any replay attacks services on the established connections between the source and destination devices while data is being transferred between them (Mahmmod et al., 2020). Furthermore, the IPSEC protocol operates in two types of modes, transport mode and tunnel mode. In the transport mode, the end points establish a secure connection by encapsulating the packet payload only. In tunnel mode all packets are encapsulated between the two endpoints to construct a VPN tunnel (Mahmmod et al., 2020).

The hypertext transfer protocol secure (HTTPS) is the secure version of hypertext transfer protocol (HTTP) (Wibowo et al., 2020). HTTP is the use for basic communication on the internet, mainly used by web browsing for access to web applications (Velagapudi & Gupta, 2019). The HTTP protocol is a stateless communication, typically working on port 80 and provides no authentication between source and destination. Since no authentication is present, this proves to be an insecure means of communicating. The user information being transferred back and forth between client and server is open to prying eyes and can lead to data theft or manipulation. A means to enhance HTTP and secure this communication for confidentiality, security

measures have been added, such as, Socket Layer (SSL) or Transport Secure Layer (TLS) into the HTTP protocol, hence HTTPS (Wijitrisnanto, 2020).

HTTPS operates by default over port 443 and uses SSL/TLS to provide a means for secure communication between client and server; with TLS being the successor to SSL. When a client request access to a web application using HTTPS, the server presents its public-keyed certificate, the client machine then validates this certificate with a Certificate Authority to validate its legitimacy and that the domain name belongs to the server. Once this is done, and no errors occurred, the client/server will then negotiate a cipher suite and a symmetric encryption key (a random bit character agreed by both parties) for the rest of their communication (Akhawe, et al., 2013). While HTTPS is not a one solution fits all for secure browsing the internet, it does reduce prying eyes from viewing confidential information, and it ensures the user is connecting to the correct web server. There are still attack vectors that can compromise HTTPS, such as browser in the middle attacks, and man in the middle attacks. Both attacks place the threat actor in between the client and server to view all communication between the parties (Wijitrisnanto, 2020). Furthermore, HTTPS is used for more than just web browser use. Any web application or means for public certificate authentication can utilize HTTPS protocol for authentication and encryption (Wibowo et al., 2020).

Authentication and Authorization

In order protect sensitive data from unauthorized access and provide accountability a system must be secured and accessed by authorized individuals. Using authentication and authorization is a basic and simple way to accomplish this task. Often

used in the same context, authentication and authorization provide different forms of validation (Anna, 2020). Authentication means validating the user states they are who they say they are, while authorization identifies what information the authenticated individuals have access to. There are a few different types of each and are discussed in below.

Username and password are authentication methods that depend on the structure and service of a system. When there is a need to maintain authorization of the data being accessed, a common practice is to require a username and password to access systems. This provides an easy and convenient way to authenticate to a system (Hossain, 2021). While this form of authentication is convenient, it is prone to various attacks, such as guessing attacks, dictionary attacks, and password leakage attacks. Security measures must be put in place to protect the database where the passwords are stored to ensure their confidentiality (Hossain, 2021).

Biometric authentication uses a unique characteristic of a user to provide authenticating. This form of biometrics can be retina, iris, finger, or voice form. This type of authentication is convenient and efficient but does have drawbacks (Sain et al., 2021). According to Hossain (2021), one possible drawback is the possibility of biometric leakage. Once the biometric characteristics have been compromised there is no way to change them as they are a unique part of the user. Hence, the biometric characteristics may no longer be used for authentication as there is no longer a way to prove the correct user is logging in.

Using biometrics or even login ID/Password provides a level of security but used independently can be a weak form of security. Combining biometrics and passwords together increases the security of confirming authentication and is called multi-factor authentication. This process of combining different forms of authentication to prove the user is whom they claim to be (Sain et al., 2021). The essence of multi-factor authentication is the process of producing *something you know* and *something you have*. In the previous examples, the something you have could be a biometric authentication, and the something you know would be the login id and password. This combination enhances the chances that the person who is authenticating, is who they claim to be.

Authorization access control becomes a critical step as the information systems retain confidential data that must maintain a certain level of integrity (Jing Gao, 2010). In the role-based access control (RBAC) authorization to data is based on the role of the individual user. This is often referenced as a security label, may be write access or even read access. This level of authorization is applied to a security level then applied to a role. All users within the role are provided the same level of access. The RBAC work well in small systems, but once a level of complexity is required, the RBAC may not provide a level of authorization to meet the complexity of the roles available (Jing Gao, 2010). In the event the complexity of the authorization must provide multi different levels based on the same roles, a mandatory access control may benefit the organization better.

Mandatory access control (MAC) is the process of controlling access to a resource through access policies (Thu Yein Win, 2014). The resources within a MAC are assigned sensitivity levels. The users of an organization are then assigned clearance levels. The

access to a resource is then defined based on the individual's clearance through access policies. This provides that a resource is not accessed by an unauthorized clearance level (Thu Yein Win, 2014).

Auditing

Auditing consists of reviewing and validating procedures and policies are in place and working. Often auditing can be referenced as IT governance which consist of certain checks and balance of the information systems that a business utilizes (Brobst & Council, 2005). Julianti (2021) stated the IT governance is the process of evaluating the risk of IT investments to increase the efficiency of managements decision-making capabilities. This can include reviewing the current systems, evaluating the efficiency and security of the system to ensure is it beneficial to the organization. One framework that is beneficial in achieving this IT governance is called COBIT. The COBIT framework is used for auditing and ensuring optimal value from IT resources (Ishlahuddin, 2020).

Log Control

Maintaining proper logging of IT systems is beneficial to IT security professionals in identifying what is occurring on their network. Reviewing logs can identify trends and anomalies through log analysis (Barabanov & Makrushin, 2021). Most common logs are event logs. Event logs are receipts of recorded actions that has taken place on the given system (Chiu & Jans, 2019). While each system is designed to generate logs for every event that takes place, the security IT professional may fine tune each system to the degree at which a log is generated. All generated logs typically comprise of four things. The activity that took place, the process instance, the resource

used, and the time the at which the event occurred (Chiu & Jans, 2019). Most collection of logs for an organization are collected and stored in a database that can be used for analytical data review such as graphs or reports (Tomono et al., 2010). By actively reviewing and maintaining proper log control, An IT security professional can actively review all processes and events that have occurred on any giving system, creating a picture for what is occurring on their network.

Physical Media Control

Controlling access to your physical systems is an important security technique that is often overlooked. System security that is designed to alert on compromise or detect an anomaly are great tools but letting anyone gain access to a physical device can prevent the advantages of having software side security (Forte & Power, 2007). When it comes to physical security all system require observation and lock down measure that deter an individual from just walking in and gaining access to the physical system. This is often achieved by creating a physical security baseline that incorporates disabled applications, restricted access, and closed-circuit televisions (CCTV). According to McCreight and Leece (2016), creating a diagram that illustrates your physical system layout can identify weak points in your physical security.

There is a trend occurring where systems are being identified using software security to ensure proper security is being applied to both the physical and software of systems (McCreight & Leece, 2016). Incorporating physical security into software security and procedures adds additional benefits that include reviewing physical security on a routine basis, including physical requirements into vendor contracts that limit the

scope of physical permitted access to limit third party access during routine visits. In recent years this has become easier for IT security professionals with the decrease in cost for implementing physical security such as IP cameras. The ability the review multiple networked cameras covering an entire area by collecting the information in one central source to be reviewed and monitored (McChesney, 2006).

User Security Awareness and Training

Computing power has increased and made access to the internet easier. According to Carella, et al. (2017), roughly 46% of the world population during their proceeding has access to the internet though some type of connected device. With the ability to access data in so many hands, user security awareness has become an increasing task for many organizations (Korovessis et al., 2017). Despite security measures an organization puts in place to prevent data compromises, the human factor is always considered the most vulnerable (Hamound & Aimeur, 2020). A user that has access to a corporate network should be trained on how and why security plays an important role when the user is accessing corporate resources.

Transition and Summary

The purpose of this study was to explore strategies used by IT security professionals for implementation of proper security practices for small financial institutions. The review of the above literature was to establish a foundation for this study and provided an overview of knowledge related to the research question. The literature review consisted of a theme approach to ensure the reader could understand the influences surrounding the topic for this study.

In the following section I focused on the project portion of this study including the rational for using a multi-case study for exploring strategies used by IT security professionals for implementing proper security practices for small financial institutions. The following sections comprise of role of the researcher, participant selection, population, sampling, data collection, data analysis, research method, research design, and reliability and validity for this study.

Section 2: The Project

In this study I explored strategies used by IT security professionals for implementing proper security practices for small financial institutions. This section of the study I discussed the purpose statement, role of the researcher, participants, the research method and design, population and sampling, data collection, data analysis, reliability, and validity.

Purpose Statement

The purpose of this qualitative case study was to explore the strategies used by IT security professionals for implementation of proper security practices for small financial institutions. The target population was IT security professionals within small financial institutions in the southeastern United States. The findings from this study may benefit IT security professionals in establishing proper security practices when securing their financial institutions network, preventing data breaches. The implications for positive social change were for a safe and secure experience for members and employees of the financial institutions when conducting business and transactions.

Role of the Researcher

In this study, I was the primary instrument for the data collection process. Pezalla et al. (2012) stated when a study has more than one researcher, inconsistent interview styles can affect the interview conversation and may affect the results of the study. For this qualitative study, I was the sole researcher and collected all the data using a semi-structured interview process. By using this process, I kept the conversation natural and

ensured the participant felt comfortable in providing as much detail as possible surrounding the open-ended questions.

My experience in IT security within the financial sector was key to understanding strategies discussed within the data collection for this study. While I work within the financial sector, I had no relationship or knowledge of the current security procedures within each participants organization. Furthermore, I had no contact with any participants prior to approval from the Walden University Internal Review Board (IRB).

In respect to the participants and ensuring my study remained within ethical standards, I reviewed and adhered to the *Belmont Report*. By doing this, I understand and followed the protocols designed to protect participants privacy and confidentiality (U.S Department of Health and Human Services, 1979). I disclosed this information to the participates prior to the interviews, so they were fully aware of how their data would be stored and protected. My goal for making sure the privacy and confidentiality was disclosed again before the interview was to ensure the participants felt as ease answering my questions throughout the interview.

There is potential for bias in any study, and this remained true within my study as well. According to Karagiozis (2018), the researcher should acknowledge and analyze the possibility of their own culturally formed consciousness to prevent projecting their own values onto the participants. The role of the researcher during an interview is active interaction that involves communicating with the interviewer, this shapes the interview by the interaction of both parties. To combat this potential bias, I performed interviews in an environment that was comfortable to the interviewer, allowing the interview to take

place as a conversation rather than an audit. Furthermore, Bergen and Labonte (2020) stated delivery and wording of interview questions may impact the tendencies for bias or unbiased responses. Taking bias into account, my interview questions were taken into consideration and focused to only represent the main research topic. I asked all questions to each interviewee in the same manner and order to keep the study consistent. I ensured any conversations outside of the response to interview questions were not considered collected data.

Participants

The participants in this qualitative study included security professionals with experience in implementing strategies for best security strategies in small credit unions. According to Ellis (2020), the purpose of the qualitative research was to answer a question in which it relates to a person's experience or interpretation of the researched question. This required that my participants had experience and knowledge of implementing security practices for small credit unions. Marshall et al. (2013) stated the selection of participants is one of the most fundamentals tasks in creating a credible research study. Thus, the participants held a position that actively employs and oversees strategies. The participant also held either a degree in information security or had related years of experience in the information security field.

My selection process for participants was based on the sampling size available within the Piedmont region of VA. Once receipt of approval from the Walden IRB, I began to reach out to credit unions within the area. I explained the significance and purpose of the study to establish a relationship with the participants. Building a

relationship with participants and maintaining professional communication establishes trust, thus resulting in the participants feeling at ease and answering the questions truthfully and accurately as possible.

Being the researcher of this qualitative study, I had to be aware of my interpersonal skills when speaking with each participant. Karagiozis (2018) stated the researcher should be aware of each participant's individuality and perspectives. This requires adaptability on the researcher's part to adjust to the participant sensitivity to make them feel comfortable and continue to build trust. I provided the participants the choice to choose the meeting place and time. Each participant chose to meet via zoom due to the COVID-19 pandemic. Therefore, I performed each interview via a recorded zoom session. I ensured that all participants were treated as IT professionals and expressed a sincere appreciation for their contribution to the study.

Research Method and Design

The three main research methods are quantitative, qualitative, and mixed method. Urban (2018), stated that it is important to let your research question determine the research method, instead of trying to alter the research question to fit the method. In this study, I focused on exploring the strategies for implementing proper security practices within small credit unions from an IT security professional's perspective.

Research Method

In this study, I used the qualitative method to answer my research question. The qualitative method is used to construct concepts in understanding social phenomena through experiences, interviews, and views of the participants (Cook et al., 2007). In my

study, I interviewed security professionals to explore strategies for proper security practices within small financial credit unions. Furthermore, qualitative methodology is not valued based on numerical results but by deepening the understanding for a specific problem that cannot be quantified (Queirós, 2017). This required collecting data from individuals' perception, stories, beliefs, and real-life experiences regarding a particular problem. In a qualitative study, once the data is collected, the data is then sorted to determine common patterns (Urban, 2008).

In my study I explored the strategies that IT security professionals use when implementing proper security practices within small financial credit unions. Qualitative researchers are interested in the experiences and perceptions from the perspective of the participants (Mohajan, 2018). Using the qualitative method, I was able to explore the strategies taken by IT security professionals at their credit unions and apply their experiences and methodologies toward my research question. The qualitative approach was used so I could take a systematical approach towards exploring my research question through the point of view of my participants within my study.

I did not choose the quantitative method for this study primarily because in quantitative studies, according to Queirós (2017), the focus is objective and the measures surrounding the study are quantifiable. Additionally, Urban (2008) stated quantitative studies are used to deal with numbers and mainly rely on a hypothesis. Because my goal was to explore the strategies used by IT security professionals to employ proper security practices, I looked for patterns and common themes. Therefore, I did not choose the quantitative method. Lastly, the qualitative method is used by researchers to explore

behaviors and attitudes toward phenomena where quantitative studies do not (Cook et al., 2007).

The mixed method combines the quantitative and qualitative method in which the researcher collects data using both methods during their study. This can strengthen the research as both methods approach the research from different views (Sawatsky et al., 2019). I did not choose the mixed method for this study as the quantitative method was not suited for this study. In mixed methods studies the data is collect by using both qualitative and quantitative methods, resulting in a statistical analysis and evaluation (Almeida, 2018). In my study, I explored different strategies that are used by IT Security professionals for proper security practices within small financial credit unions. I did not collect any statistical data and I did not form any hypothesis in this study; therefore I did not choose the mixed method for this study.

Research Design

The research design for this study was a case study. In qualitative studies the design should be primarily based on the nature of the research question (Korstjens & Moser, 2017). In a qualitative study there are various types of designs including phenomenology, ethnography, and case studies (Kalu, 2017). Case study designs are used for advancing theories by comparing similarities and differences among cases. In a case study, the sampling is not random, but chosen for its interest in the research question. Case studies are done by collecting data through interviews, archive analysis, and cross examining to identify patterns and similarities (Ridder, 2017). Furthermore, case studies can provide better understanding for the how and why things are happening within a

particular phenomenon. This is done by investigating a real-life phenomenon within its environmental context (Ridder, 2017).

According to Guetterman and Fetters (2018), a case study should be well defined on the focus and the intent of the study. The purpose of my study was to explore strategies used by IT security professionals to employ proper security practices within small financial institutions. I interviewed IT security professionals that oversee the security strategies put in place to safeguard the systems and data that are used within a financial institution. By performing a case study I explored the patterns and similarities that were used to employ what is considered proper security practices. Therefore, I chose the case study design for my research design.

In a phenomenological design, a researcher explores the human aspects of the lived experience, digging into the emotions, sensations, and perception of the experience (Wilson, 2015). In my study, I did not focus on individuals' perceptions of experiences, but the strategies IT security professionals use to implement proper security practices within small financial institutions. Therefore, I did not choose the phenomenological design.

According to Reyes (2018), the ethnography design differentiates from other designs as the researcher uses environment and culture surroundings to understand lived experiences. I did not choose the ethnographic design as I did not focus on environments or culture surroundings. I explored the strategies implemented by IT security professionals for proper security practices within small financial institutions.

Population and Sampling

In the following sections I discuss population, data sampling, data saturation, and how they applied to my study. According to Berndt (2020), the population is composed of the individuals that possess the information desired by the researcher in relation to their study. In my study, the population included IT security professionals that oversaw or implemented security practices employed by small financial institutions. Additionally, the institutions operate or offer field of membership within the Piedmont region in VA of the United States. IT security professionals were the target population as they possessed the skills and knowledge for answering research questions surrounding strategies for proper security practices within their organization.

In a qualitative study there are different strategies for data sampling including: convenience, snowball, and purposive sampling (Gill, 2020). My study was to explore the strategies used by IT security professional for implementing proper security practices within their small financial institutions. To answer my interview questions accurately, I needed the participants to understand their organization's security and infrastructure. Therefore, I chose the purpose sampling technique for my study. Palinkas et al. (2015) stated that purpose sampling technique is used by the researcher to choose the participants based on the value of information the participant can provide to ensure the study consists of valuable information when limited resources are available. Etikan and Bala (2017) stated this type of sampling may also be referred to a judgmental sampling, because the researcher picked and chose the participants that provided the best information for the study. By choosing qualified candidates for this study, I was able to

ensure that all participants held the knowledge and expertise for answering my research questions regarding their strategies and decisions for employing those strategies.

Data saturation depends on the researcher's sample size and strategies. To ensure data saturation is reached, the researcher first must be able to collect quality data from a sufficient sample size (Gill, 2020). Peterson (2019) stated in qualitative studies, the focus should be on a small number of participants that when selected can provide deep information to the cases. Therefore, for this study, I selected three participants from three different organizations. According to de Cassia Nascimento et al. (2019), data saturation is then obtained when no new information is provided and the information from participants starts to become redundant. In a qualitative research study, one way to obtain data saturation is to perform semi-structed interviews with open-ended questions. Bernard (2012) stated the number of interviews to justify saturation is not quantifiable, by using the same open-end questions on each participant, the researcher can reach data saturation. The plan for achieving data saturation included collecting data through multiple sources, or as stated in Fusch and Ness (2015), data triangulation. Data triangulation goes hand in hand for reaching data saturation. Once all data was collected and compared, to further attain data saturation, I performed member checking as well.

The interview process and member checking took place in a comfortable setting agreed to by the participant. The participant interviews were one on one to ensure answers to the open-ended questions were not influenced by anyone. The interviews were either over the phone or in person depending on how comfortable the participant was.

Follow up member checking was done by email to ensure the participant agreed with my interpretations of the conversation.

Ethical Research

Once consent was granted from the Walden IRB, I reached out to participants via email to make them aware of the opportunity to participate in my study. The email included an introductory summary about myself, a summary of the study, a consent form, the interview questions, and my contact information. The following sections discuss the consent form, rights of the participants, incentives, and protection of participants and data.

Informed Consent

In qualitative research ethical principles must be taken into special consideration to ensure the protection of the participants (Arifin, 2018). Furthermore, informed consent should provide detail of the study, and allow the participant in a voluntary state decide whether to participate or decline (Sullivan, et al., 2021). The consent form for my study consisted of (a) the purpose of the study, (b) the role of the participant in the study, (c) role of the researcher in the study, (d) data confidentiality, (e) intention of publication of study, (f) incentives, (g) withdraw process. All participants were provided a consent form and agreed to and signed the consent form prior to participation.

Rights of the Participants

Protecting the participants rights is the top priority and should ensure the participants dignity, rights, and safety to into account when it comes to ethical research (Van den Hoonaard, 2008). This study included no personal identifiable information, and

all participants privacy were respected throughout the research process. The participant also had the right to withdraw from the study at any time and their data would be properly discarded.

Incentives

In my study no participants were given any type of incentive for participation. Hsieh and Kocielnik (2016) stated the introduction of incentives may provide a risk of bias input, as adding incentives can alter who ultimately decides to participate. However, this influence may be small, so to completely rule out the potential, no incentives were provided. I clearly stated this on the consent form to ensure all participants were participating voluntary with no exceptions of rewards.

Protection of Data

My study followed the Walden University IRB ethical and legal requirement procedures to verify no harm or risk came to participates that volunteered my study. One of the responsibilities of a researcher is assuming role of the data holder. The data holder must take proper precautions to protect the data collected during the research process. Mckibbin et al. (2021) stated one way to do this is by removing identifiers about the participants. By removing identifiers about the participants and organizations, I was able to ensure that each participant and the organizations in my study remained confidential. According to Coffelt (2017), when participates are assured about confidentiality, they are more willing to participate within a research study. Thus, each participant and organization within my study were assigned unique identifiers during the data collection process such as P1, P2, etc. These identifies corresponded with a key that was password

protected in a sperate data file only accessible by me. Lastly, all data was secured and met the IRB guidelines specified by Walden University. The data resided in an encrypted file container on my PC that required a password and a key file to decrypt. The key file is stored on a separate drive and backed up to an external USB drive. Once the five-year time span has been exceeded, all data and its contents will be properly sanitized using Department of defense standards. This will include all data including documentation, contacts, research, and recordings.

Data Collection

Data collected in qualitative research greatly depends on the researcher and their approach to sensitivity, environment settings, and methodological skills (Yildiz, 2020). The types of tools that are used for data collection are observation, interviews, and document analysis (Yildiz, 2020). In this multi case study, I utilized data collected from semi-structured interviews, documents provided from participants, publicly available documents, and my own observation from the participants. In the following sections I discuss the data instruments, collection techniques, and organization techniques that were used in my study.

Instruments

In qualitative research, the researcher is the main instrument for collecting and analyzing the data (Clark & Veale, 2018). In this study I was the main instrument for collecting data. The data collected from researched documents surrounding proper security practices and through semi-structured interviews with IT security professionals that occupy the role for designing and implementing security practices within small

financial institutions. Yildiz (2020) stated the role the researcher plays in qualitative research is more than just interviews and reviewing documentation. The researcher, being the main instrument, must relate to the participants, be in their setting, and understand what the participant means to evaluate the information correctly (Yildiz, 2020). My understanding of the research topic in relation to the conceptual framework was important for processing and collecting of the information that was expressed from the participants.

Heath et al. (2018), suggest that in a qualitative research topic that are sensitive in nature, a good rapport is important. Furthermore, making the participants relaxed and comfortable so that the participant can explain complex scenarios and the researcher understand them, this provided better quality conversations regarding the research topic. While I was the main instrument in the study, I retained my role as the researcher and limited my bias by letting the participants to speak freely. According to Moser and Korstjens (2018), it is important to limit my guidance on answers and prevent answers from being influenced to fit my perspective. By allowing the participants to speak freely, I was able to ensure all data was collected accurately during the interviews.

The interview process for my study was accomplished by performing semi-structured interviews and following an outlined interview protocol (Appendix A). According to Aborisade (2013), the strength from using qualitative research is from performing interviews that provide in-depth investigations into the research topic. The most common type of interview is the semi-structured interview (Dejonckheer & Vaughn, 2019). In semi-structured interview, the process follows an outline of topics and

questions created by the researcher, but the flow of the conversation can go beyond the outlined questions depending on the interviewee's responses and the follow-up questions that come after. This provides the researcher opportunity to gain in-depth investigation regarding the subject matter (Adhabi & Anozie, 2017). Additionally, semi-structured interviews are not the only type of media available. According to Aborisade (2013), data provided by participants can be provided in forms of documents such as policy and procedures. All the documents and interview responses were collected as data to then analyzed toward my research question. Lastly member checking was used against all received material to clarify all responses and intentions were received in the correct context.

Member checking is the process of validating the researchers' interpretations by allowing the participant the opportunity to review the responses obtained and interpreted by the researcher (McGrath et al., 2019). All participants were provided an opportunity to review their responses to the questions asked during the semi-structured interviews during a follow-up session. This provided the participants the chance to validate their responses and ensure the data interpreted remained creditable. According to Candela (2019), the purpose of member checking allows for accuracy of interpretations formed during the interviews with participants. Additionally, Yin (2014) stated follow up sessions also provide the participant with the opportunity to add on any new evidence that may have been forgotten or misinterpreted.

Data Collection Technique

The collection of data for this study was obtained by reviewing documents provided by participants and conducting semi-structured interviews. The semi-structured interviews followed an outlined interview protocol (see Appendix A). According to Yeong et al. (2018), a reliable interview protocol is vital for not only securing quality data but ensuring the researcher can obtain as much data within an allocated timeline. Secondly, an interview protocol helps the researcher prepare and according to Van de Wiel (2017), ensures the interview is conducted in a standard manner. Furthermore, the interview protocol was used as a roadmap instead of strict guide. Arsel (2017) stated the interview protocol is treated more as a checkpoint when conducting semi-structured interviews. The conversation between researcher and participant is different each time and the flow of the conversation may need to be tailored depending on the participants answers. Furthermore, Arsel (2017), stated by doing this approach you are allowing your participant the freedom to express their own views and expertise toward the matter, resulting in quality data.

Each interview took place in a location chosen by the participant and was conducted following the interview protocol (see Appendix A). A recording device was used in the interview process to ensure playback and transcribing later was possible. The collection goal was to ensure the participant felt comfortable and were at ease to answering all the open-ended questions (see Appendix B) in an accurate manner, resulting in a fluid conversation regarding the research topic. Using open-ended question promotes further in-depth conversation by allowing the participant to freely express their

views and experience regarding the research topic. According to DeJonckheere and Vaughn (2019), the purpose of a semi-structured interview is to learn about the participants expertise in the topic of interest, including experience, attitudes, and perceptions. By using open-ended questions that were clear and precise I was able to obtain rich quality data.

Member checking was completed to increase reliability and validity of the data. I cross examined all documents provided by the participant along with transcribing the interviews conducted. Livari (2018) stated member checking provides an opportunity for the participants to check the researchers work and validate their responses. This leads to better validity and increased trustworthiness of the research. A follow-up session was held two weeks after the initial interview where the participant had the ability to review my interpretations of the interview by receiving a copy of the completed analysis to review and confirm their accuracy. According to Candela (2019), this provides the participant the chance to review their responses and provide additional feedback or potentially contribute new evidence to the study.

Once IRB approval had been completed and approved, I reached out to potential candidates and started the interview process. The step-by-step process is below:

- IRB Approval
- Invitation to potential candidates is emailed
- Interviews are scheduled and consent forms are signed
- Interview is conducted using interview protocol and questions (see Appendix A & Appendix B)

- Interviews and documents provided are transcribed verbatim
- Member checking occurs
- Follow up session to provide copies of interpretations and finalize member checking
- Finalization of data analysis

Using interviews as the data collection technique for qualitative research had both advantages and disadvantages. Some of the challenges researchers might face when conducting semi-structured interviews is the amount of time it requires. According to Barrett and Twycross (2018), transcribing an interview can become a time-consuming task where a one-hour interview might require up to five or six hours to transcribe. Another disadvantage of semi-structure interviews is identification for bias.

In Johnson et al. (2020), the researcher must be aware of their own bias that might affect the data collection process. The researcher needs to be aware of their body language, facial expressions, etc. How the researcher presents themselves in front of the participant may alter how the interaction between participants and researcher conveys. Lastly, in addition to researcher bias is the unintentionally bias in data collection. The researcher must focus and acknowledge their own bias toward the research topic to prevent from altering the data responses from participants.

Peterson (2019) stated the researchers' reactions to responses that participants provide, needs to remain neutral. If the researcher relates to closely with their own experiences or views, then it may affect the data collection process. This potentially can affect follow-up questions, data analysis or even causing misinterpretations of data.

Following the interview protocol and performing member checking reduced the potential for bias and ensured I stayed on schedule.

I discussed a few of the disadvantages for using semi-structured interviews as the data collector, but while there are some disadvantages, there are also advantages to using this type of tool for data gathering. Diefenbach (2009), explained that interviews uncover ideals and insight that other methods do not. During interviews, open-ended questions provide the interviewer the chance to provide details about their experiences, insights, and feelings (Ballena, 2021). Additionally, interviewing provides a researcher not only verbal, but non-verbal responses from the participants which steers the conversation (Van de Wiel, 2017). Lastly, semi-structured interviews provide a researcher the chance to follow up on responses from the participants by asking follow-up questions and engaging the interviewee for further explanation to enhance responses (DeJonckheere & Vaughn, 2019).

Data Organization Techniques

The data collected from each interview were captured by video conferencing software and notes were taken by me to summarize each response. Irani (2019), stated videoconferencing has become a popular data collection technique since it breaks the constraints on schedule, geographical, and time. This option was provided due to the Coronavirus pandemic where some participants are still not comfortable meeting face-to-face. If the participant were comfortable meeting face-to-face and would like to do so, then a voice recorder was used instead of videoconferencing software. Along with a voice recorder, I kept notes and logs of observations during the interviews. According to

Renz et al. (2018), in qualitative studies it is typical for the researcher to utilize logs, notes, and recordings to capture the data during the study for later analysis. Lastly, data was stored and analyzed using the Nvivo software. This application keeps all data and information pertaining to my study in one central location.

The data collected in this study was transcribed into Microsoft Word and then uploaded into QSR NVIVO software tool. Each participant was assigned an alphanumeric code that masked their identity. The pseudo randomization followed a simple form and corresponded to each participant. The key for correspondence was stored separately and requires a password for unlocking.

The electronic data that was obtained throughout this study was encrypted and stored on my computer hard drive utilizing VeraCrypt container. The container required not only a password for decrypting, but also an electronic key file. The VeraCrypt container file was backed up onto a USB drive and stored for safe keeping. All other documentation and notes were stored in a small locked safe and proper stored away. Once the five-year period is up all documentation and encrypted file containers will be destroyed.

Data Analysis Technique

In this section I discussed the process for analyzing the data collected through the semi-structured interviews. According to Archer (2018), data analysis is the process for analyzing data collected from the data collection process by sorting and breaking that data up to identify themes and patterns. In this qualitative study, I used the thematic analysis approach for the data analysis. Lester et al. (2020) stated a thematic analysis is

sometimes considered an umbrella for data analysis as it is widely used and a flexible analysis technique. Mackieson et al. (2019), describe thematic analysis as more than just describing data that is collected but requires the researcher to add intellectual contributions while interpreting the data, leading to an extraction of patterns or themes within the data. Lastly, Neuendorf (2018) stated in thematic analysis there is a six-step process that is followed: (1) familiarizing oneself with the data, (2) generating codes for categories, (3) searching for themes, (4) reviewing themes, (5) defining and naming themes, (6) producing a report. Each step is described in detail below.

The first step was familiarizing myself with the data. I reviewed all data collected through the semi-structured interviews including any documentation that was gathered during that time. I went over any provided documentation, interview notes, and researched general practices that my participants stated were implemented by their organizations for creating codes and categories in the next section. Since my study involved proper security practices for small financial credit unions, reviewing and looking at general best practices was key in correlating the practices used by the organizations compared to general best practices. I took notes and highlighted general comments through the review of the data to prepare for the next step. Lastly, in this step I transcribed the interviews into a Microsoft word document. This helped me in getting familiar with the data, as Lester et al. (2020), suggested transcribing helps the researcher deepen their understanding of the participants' responses.

The second step in the data analysis involved generating codes for categories. I accomplished this by creating codes from distinctive words, phrases, or comments. I

imported all transcribed interviews into a software application for transcribing and identify codes. The software I used is the Nvivo application. This application is useful in identifying codes and patterns from the imported interviews. Akinyode and Khan (2018) stated coding consists of tagging information that relates to the overall research subject and can produce themes or patterns from the data.

The third step involved looking for themes and patterns. In this step, I reviewed the codes and categories that were labeled and tried to see if any themes or patterns could be emerged from the data. This was completed by comparing the categories to see if there were similarities or differences and reviewing codes for references to other codes. The purpose of this was to try and identify any patterns or themes that might be visible from the cross comparison. In general, Lester et al. (2020) stated the themes should align with the conceptual framework of the study and help understand the primary research topic.

In the fourth step all themes were reviewed and re-examined to see if I could identify any new themes that were smaller themes outside of the main research question. According to Scharp and Sanders (2018), the fourth step is to not only re-examined for any new themes, but verify existing themes work compared to the coding and data sets. During this step I looked at the patterns identified by the Nvivo application and reviewed to see if I was able to discover other themes that may have not been considered initial but arose from my coding and category cross comparison.

The fifth step of the thematic analysis process was reviewing my discovered themes and naming them. Once I crossed examined and reviewed each possible theme, I reviewed how each theme correlated to my study. This ensured I was only working with

themes that were relevant to my study and provide my results with valuable information. According to Byrne (2021), naming themes requires a deep analysis of the data sets. In this step the themes and the data sets that support the theme were used for the next step. Each theme should consist of supporting data sets that can explicitly support the theme. Furthermore, Herzog et al. (2019) suggested defining themes as the story that has emerged from the data and how it relates to the overall research topic.

The six and final step consisted of me writing up the report from the findings. This involved extracting portions of the data that were used in my report for evidence of my themes. According to Herzog et al. (2019), the extracts may be references or quotes from interviews but should support the overall themes. Additionally, Herzog et al. (2019) stated while the report is produced in step six it is started at step one and progressively builds throughout the entire process to illustrate the study findings in a final narrative.

Lastly, I performed methodological triangulation for reliability of the coded themes and patterns. According to Dzwigol (2020), triangulation is an important factor for ensuring reliability when interpreting data from different sources. In methodological triangulation Abdalla, et al. (2018) stated there are more than just one method of obtaining the data, such as interview and observation. In my study I conducted semi-structured interviews then reviewed any publicly available or provided policy and guideline documentation by my participants. By using triangulation, I was able to enhance confidence and validity in my results.

Reliability and Validity

Reliability

According to Spiers et al. (2018), reliability and validity of a study are incorporated to prove data adequacy and data appropriateness. In this study I achieved reliability by providing my participants with a copy of the transcribed semi-structured interviews to ensure my interpretation were accurate and correct. Livari (2018) stated member checking provides an opportunity for the participants to check the researchers work and validate their responses. This ensured that the data interpreted was concise and adequate for my study. Additionally, I performed methodological triangulation with available documents compared to responses. Santos et al. (2020) stated in qualitative studies, using triangulation provides credibility to the study by involving multiple data sources to provide multiple perspectives. Using methodological triangulation to cross reference interview responses with observation and additionally any provided policies, guidelines, and regulations strengthen the data confidence in my study. Lastly, data saturation was used to fulfill reliability and validity. According to Hayashi et al. (2019), data saturation occurs when no additional useful information is being provided from interviews.

Dependability

Scharp and Sanders (2018) stated dependability refers to how the researcher shows they came to their findings. Additionally, Nassaji (2020) suggested dependability ensures that data is reported in a manner that if reviewed by another researcher, they would conclude similar interpretations from the data. In my study I achieved

dependability by performing member-checking throughout my study. I provided all participants the chance to review my interpreted data during follow-up interviews to ensure their answers to my questions were interpreted correctly. This ensured each participants responses were transparent and accurate throughout my study. FitzPartick (2019), suggest when the researcher performs member-checking by providing their transcripts to the participants for feedback, they are confirming credibility by having the participants validate the interpretation and transcripts.

Creditability

Haven and Grootel (2019) stated a researcher's creditability is strengthened by the foundation from which a conclusion is drawn on. In my study I built creditability by using triangulation and performing member checking. Methodological triangulation was performed on all policies, guidelines, or procedures produced during interviews. As noted by Santos et al. (2020), triangulation is a strategy used in qualitative research to not only increase the credibility but to also the understanding of the research topic. Furthermore, Lemon and Hayes (2020) stated triangulation is used to strengthen creditability and reliability by reducing systematic bias, improving the findings in a study. I reviewed all collected information and cross-examined responses with any available documents establish trustworthiness within my collected data.

Member-checking also took place after initial interviews. According to Stenfors et al. (2020), one method of enhancing creditability is to provide the preliminary findings to participants for confirmation and elaboration. I performed follow-up interviews with each participant. This provided the participant a chance to review my interpretation of their

transcripts, along with my initial transcripts to ensure data accuracy. Member-checking also allowed the participants an opportunity to elaborate more on any responses they felt were in adequate, leading to more thorough responses.

Transferability

Amin et al. (2020) stated transferability is the aspirational result for researchers in a rigorous qualitative study. According to Peterson (2019), to ensure transferability, it is the researcher's job to provide as much context about the study to provide other researchers the ability to replicate the study. This includes but not limited to participants, data gathering, and data analysis. In my study I provided detailed information for readers about participants settings, location, data analysis procedures, result finding, throughout my study. By doing providing this information, I ensured transferability is applicable to any reader or researcher looking to transfer my study into their own context. Lastly, Nassaii (2020) stated transferability is not for the researcher to make any generalized claims, but to provide enough detail of their study that readers are able to transfer the study into their own context if necessary.

Confirmability

According to Nassaii (2020), confirmability is accomplished by providing audit trails for all data and findings in a study. As stated in Eldh et al. (2020), being able to follow the entire research process is vital to validating confirmability. In my study, I provided an audit trail by keeping logs and notes of the data collection, data analysis, and accompanied by member checking. I provided my participants the opportunity to check my interpretations of their responses and to ensure their responses were accurate. I also

reviewed research logs throughout the research process to limit researcher bias by ensuring I'm followed proper steps in the research process.

Data Saturation

Aldiabat and Le Navenec (2018) stated data saturation is crucial as it determines a complete study and the depth of the data collection and analysis. Furthermore, Moser and Korstjens (2018), stated that sampling should occur until saturation is reached, which is determined when no new analytical information arises. In my study I determined data saturation when no new information was identified from interviews or documents obtained during the interviews. Once data saturation had been determined, I verified and examined all information for accuracy, which I accomplished by performing member checking. FitzPartick (2019), suggest when the researcher performs member-checking by providing their transcripts to the participants for feedback, they are confirming credibility by having the participants validate the interpretation and transcripts. Once member checking was complete and all data obtained had been verified, I was able to ensure data saturation has been achieved.

Transition and Summary

In section 2, I covered the main purpose for my study, the research design, the research instruments, participants, sample size, and validity for my study. The purpose of this study was to explore strategies for proper security practices within small financial institutions. I chose the triangulation methodology for validating of this qualitative study. Section 3 is comprised of the research findings and their relative themes. Additionally, I

covered applications for professional practice, implications for social change, offer recommendations for future research and action, and reflections.

Section 3: Application to Professional Practice and Implications for Change

In my study I explored strategies used by IT security professionals for implementation of proper security practices for small financial institutions. In this section, I present findings from my data collection and data analysis. Furthermore, I discussed the potential implications for social change, recommendations for action, potential for future research, and a final reflection on my study.

Overview of Study

The purpose of this qualitative multiple case study was to explore proper security practices by IT security professionals within small financial institutions. I obtained the data for this study by conducting semi-structured interviews with three participants. Each participant held a senior position that oversees implementations of security policies or worked directly with reviewing and applying security policies within their financial institution. The participants were in the Piedmont region of VA within the United States. I performed member checking with each participant after the interviews were transcribed to validate my interpreted transcriptions reflected each participants responses corrected. By performing member checking, I ensured the participant had the opportunity to validate or correct any interpretations if they were transcribed inaccurately. Finally, I performed triangulation by comparing participants responses with public documents available to strengthen the creditability of the study.

Four major themes emerged during the thematic analysis portion of this qualitative multi-case study: (a) layered security, (b) security auditing, (c) technology adaptative, and (d) vendor management. Each theme that emerged relates and builds on

existing literature I discovered during the literature review. The findings also align with the TAM which was used as the conceptual framework in this study.

Presentation of the Findings

The research question I used for this study was: What strategies do IT security professionals take to mitigate security vulnerabilities for their small financial institutions? In this study I explored three organizations in attempt to answer my research question. The data came from three IT security professionals each from different financial institutions. All participants oversee security practices that involve management, mitigation, and implementation of security policies and practices. After I completed the initial interview with each participant, I transcribed the interviews and then performed member checking with each participant. Lastly, I uploaded the transcriptions into NVIVO software for thematic analysis.

In the following section, I discussed the four major themes that were discovered during the thematic analysis. The major themes that emerged from this study were: layered security, security auditing, technology adaptive, and vendor relationships. I tied each theme and their subthemes back to the information presented in the literature review and the TAM conceptual framework that I was used for this study.

Theme 1: Layered Security

The first theme that emerged in the thematic analysis was layered security. According to Vijayakumar et al. (2022), organizations must take a multi-layer approach when it comes to security. This can be achieved by implementing network security systems that align with defense standards and requirements. The responses I received

from the participants aligned with the information identified in the literature surrounding security tactics to achieve multi-layer security approach. Table 1 shows the references related to the theme layered security approach.

Table 1

References to Layered Security

Major Theme	Participant Count	References
Layered Security	3	29

A multi-layer approach is achieved by implementing procedures and tactics in place. This can involve placing applications in a DMZ. P1 explained their organization falls within an umbrella of a parent organization and one tactic in place is segregation. By P1 having network seclusion provides them the gain of additional security within their parent network but also secludes them to be their own separate network.

The use of VPN is another tactic in a multi-layer approach. Each participant in this study confirmed to using a VPN when handling remote users for internal access. Controls for VPN access are set in place to limit who and when a user can connect to the network, requiring an administrator approval according to P3. Participant P2 limited users based on position within their organization for having the ability to connect remotely through VPN connections. Each participant affirmed that only company issued devices were allowed to connect via VPN. This ensures the devices meet and maintain company standards for security assurance.

Aligning with the use of VPN connections for remote and external users, all participants affirmed to using some type of MFA. P1 discussed requiring MFA to connect

to internal services, while P3 explained that users must initiate and follow an MFA process to successfully obtain a VPN connection. This provides an extra layer of authentication to verify the user prior to allowing access to the internal network. Due to the Coronavirus pandemic, workers needed a way to work remotely. P2 accomplished this by providing company issued devices to employees for working remotely. However, as the pandemic has started to come to an end, the need for remote work has reduced. P2 removed some remote workers access and revised their policies to include remote work based on individual roles within the organization. This requires users, depending on their role, to come back into the office. While P1 and P3 performed similar tactics during the pandemic, both P1 and P3 have embraced remote work and continue to have more flexibility with remote work due to the security controls put in place prior to the COVID-19 pandemic.

Security controls are a combination of policies and procedures that limit or reduce risk to the organization. All three-participants suggested controls such as hardening checklists for machines, limiting the machine to perform certain functions while external to the organization, implementing network access control. Each control and policies combined creates a multi-layer approach. P3 stated, “Think about the attack surface, there are certain strategies for somethings, and there are certain strategies for other things. The idea being that you know all those different attack vectors then you assess your risk to them.”

A common technique for identifying attack vectors that was expressed by all participants is vulnerability scanning. Each participant explained they perform scans of

their networks and devices connected to those networks. P1 expressed that performing scans identify the holes and weakness in a network. P2 expressed the importance of scanning items such as hardware equipment or software to identify weaknesses. After a scan, IT professionals should review the results and mitigate where possible. P2 suggested rescanning after mitigating a vulnerability to ensure the mitigation is in place. Of course, this is not always the case, some fixes may cause a disruption to a business, or a fix is not available due to vendor limitations. Each risk must be reviewed to see what additional options are available to reduce the risk to an acceptable level where the risk could be accepted according to P2.

All three participants expressed to having multiple security layers in place. The data collected from the semi-structured interviews and review of public documents illustrate and support the theme of layered security. Therefore, layered security is an important strategy for IT security professionals when implementing strategies for proper security practices within a small financial institution to prevent security breaches.

The findings of this study support layered security and are present in existing literature. According to ALSaleem and Alshoshan (2021), in a secure environment, authentication determines whether a person should have access to a system or not. Each participant expressed to not only require authentication, but by implementing multi-factor authentication. This creates an additional level of security as a potential threat actor must break all authentication factors as opposed to just the username and password in a single factor fashion. Additionally, layered security constitutes implementing strategies such as policies, procedures, and processes to limit risk, as suggested by P3. Jackson and

LaTourrette (2015) stated layered security can be thought of as a block of swiss cheese, where each slice is peppered with holes, no one hole will lead you through the entire block of cheese. Each participant spoke to having multiple controls in place to supplement risk for their environments and acknowledged that security is a multi-layer approach. All participants suggested using appliances such as firewalls and intrusion prevention systems.

A firewall will either pass or block traffic based on the set of rules implemented by an organization when receiving or sending traffic. Thus, Alvarez et al. (2021) stated firewalls can prevent malicious traffic from entering or exiting a network. According to Wang (2017), IPS and IDS are considered a second line security defense and are typically placed behind firewalls and reside either internal or within a DMZ. The literature that I reviewed aligns with the findings of the study, when an IT security professional uses a combination of different security techniques, the result is a layered security approach.

Recent literature continues to support the theme that layered security is an important strategy for IT security professionals when mitigating security vulnerabilities for their small financial institutions. Mukdasanit and Kantabutra (2021) stated layered security is the practice of implementing a series of defense mechanisms in place if one mechanism fails or is compromised, another mechanism will be in place to thwart the attack. Layered security can be compared to the roots to a tree, a tree has many different roots grounded to prevent it from easily being knocked over. According to Mukdasanit and Kantabutra (2021), organizations that are using technology to provide channels from

outside the organization to internal resources must consider the vulnerabilities and attack vectors.

While not all threats can be eliminated, a threat actors' footprint can be reduced when an IT security professional uses a layered security approach. Layered security may also make it more difficult for a threat actor to further their attack by facing multiple different security mechanism. According to Petroia and Banu (2019), having multiple security mechanism in place may provide an IT security professional more time to detect and contain threat potentially reducing the amount of data compromised.

The next section I discussed the findings in correlation to the conceptual framework, TAM. IT security professionals are faced with cumbersome issues in that they must provide sufficient security policies to protect IT infrastructure, but also make the systems usable enough for employees to affective perform their jobs. According to Hanif and Lallie (2021), the TAM assess the acceptance and use of technology by individuals. When there is a lack of knowledge about a technology, a perception is conceived that it is difficult or too complicated to use.

As noted by P3, a big part of the conversation with people is that it isn't about policing you, it is about protecting the network. According to Siwale (2022), TAM depicts the use of technology from the behavioral intention which is derived from the attitude toward technology and perceived usefulness. The strategies used by IT security professionals to implement proper security practices to prevent security breaches are connected by ensuring the technologies chosen are easy to use but effective in securing the organization. According to Alassaf and Alkhalifah (2021), IT security professionals

must not only focus on providing a sufficient security posture for the organization but have policies in place that don't over complicate the user experience in a way that prevents using the technology. All participants mentioned that user feedback was important to their organization when implementing new technology.

Theme 2: Security Auditing

The second theme that emerged during the thematic analysis was security auditing. Security auditing is vital when it comes to organizations' IT security posture. Matsikidze and Kyobe (2020) stated one of the main responsibilities in auditing is to identify risks, vulnerabilities, and detect where proficiencies can be made to strengthen an overall IT security posture. The responses gathered from the semi-structured interviews aligned with information found within the literature regarding tracking, assessing, and reviewing security. Table 2 below shows the frequency in which the theme was drawn.

Table 2

References to Security Auditing

	Participant	
Major Theme	Count	References
Security Auditing	3	56

In the security auditing theme, there were four main areas: policy review, tracking, testing, and training. Organizations are often changing policies and procedures based on trends or technology changes. According to Robertson (2012), security policies and procedures are the necessary components that govern how organizations' system should be used; ultimately attempting to protect resources on the systems. All three

participants expressed to reviewing policies and procedures on a regular basis to make sure their respective policies are sufficient in meeting their organizational needs. P1 expressed to reviewing top level organization policies such as the Information Security policy at least on an annual basis. While P2 works with a third-party vendor to assist in reviewing and updating their policies. According to Djerouni (2019), auditing policies and procedures should be performed at least annually to validate their accuracy and effectiveness regarding security for the organization.

One technique for auditing systems is when an IT security professional cross examines user actions with established procedures to determine a security policies effectiveness. Each participant acknowledged reviewing access logs based on time and destination to ensure users were accessing systems within designated time frames. P2 noted this as a process for keeping eyes on the network by monitoring IPS and Firewall logs, reviewing user login activity. This type of auditing identifies and can show if a user is accessing systems outside of designated authorized time, which might be a sign of a compromised account or intent for misuse of company resources; a big brother monitoring mentality as mentioned by P1. P1 also noted that it is the same processes for vendors, checking up on vendors access logs, making sure the vendor is sending out notifications and that the vendor is doing security updates on their end to protect their systems as well.

Tracking security trends such as zero-day attacks, current events, and technology innovations require organizations to review and add policies on a regular basis. All participants acknowledged the importance in keeping up with current trends and

vulnerabilities that affect their organization. All three participant expressed that one of their sources for information gathering on new vulnerabilities and trending threats were vendors that each organization had relationships with. Furthermore, P2 discussed being part of a security group consisting of other financial institutions that meet monthly to discuss current trends and threats. Lastly, all three organizations discussed getting alerts and threat updates from U.S Computer Emergency Readiness Team (CERT). Using news sites, government agencies, and vendors to stay abreast to new threats ensure IT security professionals are current on trending activity. In combination with being informed of trending threats, is correlating those threats to risks toward the organization. This typically can be accomplished by using security appliances such as a vulnerability scanner.

P1 described running a patching appliance on internal systems to identify vulnerabilities. Once a vulnerability is known it can then be mitigated on a test system to ensure no other systems are interrupted by the patch. Once verified, the mitigation patch can then be applied to production equipment. This process for tracking vulnerabilities was also present in P3 by using internal scanning systems to stay current on vulnerabilities within their infrastructure. IT security professionals rank and track all discovered vulnerabilities with the critical vulnerabilities be worked first. By performing this type of security auditing, the organization can eliminate the top security concerns first and then focus on the lower severity vulnerabilities based on organization need. Furthermore, security auditing typically involves more than just the IT security

professional reviewing policy or procedures, security auditing can also involve testing systems and people in real world scenarios.

Disaster recovery testing, penetration testing, and user testing are used by an organization to identify gaps that should be addressed to better prepare for a real-world scenario. Srivastava (2021) stated the more an organization practices the better prepared they can be during a real event. According to Thomas et al. (2019), most penetration testing consists of rules of engagement that are defined and set by the penetration vendor and the organization. The main objective for penetration testing is explained by P1 where the tests are performed to identify holes and weaknesses within systems. Once discovered, the organization can review them and create policy and procedures that limit the risk. Each risk is different and not all risk can be eliminated but the goal is to reduce the risk to an acceptable limit comfortable by the organization as noted by P3.

Disaster recovery according to El-Temtamy et al. (2016), is the process for keeping a business going forward despite disruptions. Organizations need to plan for system failures, natural events, and malicious event scenarios that can occur outside of the organizations control. P3 suggested performing at least annual testing of disaster recovery where systems are brought online and verified the system can function properly. Additionally, P1 stated system recovery should be tracked for how long it takes a system to be fully functional from a restore. Ramesh et al. (2023) stated tracking the time to recovery provides metrics for what an organization can expect from when a system goes down, to when the system will be fully functional again. According to Hu (2019), it is necessary to analyze computer detection, maintenance, and data recovery. By restoring a

system from backups, the organization can test redundancy and resiliency of their infrastructure. Testing is not only exclusive to systems but can be used for employees as well.

User testing and training is often viewed as user security awareness training. It is important to test users about their security knowledge to prevent unauthorized access to an organizations' system. Carella et al. (2017), stated no matter how secure a system or device within a network is, there will always remain an easy vulnerability – users. Each participant acknowledged to performing user awareness training at least annually along with performing phishing campaigns against their users. Email is an easy communication channel for threat actors to send links that may contain malware or fake websites that can result in attacks such as credential harvesting. By performing test phishing campaigns an organization can provide real-world examples for training users. P1 noted their organization actively informs users they are testing them to increase more aggressive screening of emails and calls and P2 implements security awareness proficiency tests that identify training gaps for users upon completion. Training users is a first line of defense for most business as a user typically has direct permissions for accessing systems to perform their job function.

The literature supports the theme for security auditing as a key strategy for implementing proper security practices within small financial institutions to prevent security breaches. The findings in the following studies correlate with the responses of the participants to the interview questions. According to Zhou (2020), the main purpose for auditing is to reveal information security risks and economic risk caused by defect in

systems. Thus, promoting stronger controls for internal management, strengthen overall information system security. Additionally, auditing consists of reviewing and validating procedures, policies are in place and working. According to Brobst and Council (2005), auditing can be referenced as IT governance that performs a certain checks and balance of the information systems that a business uses. This provides an IT security professional the ability to not only identify new risks but evaluate current procedures to identify their effectiveness in controlling access to sensitive systems.

According to Robertson (2012), auditing is used by IT security professional to find policies that are lacking or inappropriate and need revisions to better align with company strategies. Policy and procedures are the guidelines for how IT security professional enforce user interaction with systems. Each policy or procedure must align with an organizations expectation for how they want a user to access and interact with a system. By performing audits such as log reviewing, penetration testing, and policy reviews an IT security professional can adjust their policies and procedures to tightly align them with security standards to safely protect systems, which is the goal of security auditing.

In more recent literature, the security auditing theme is further supported when it comes to proper security practices for small financial institutions for preventing data breaches. Xing (2022), stated security auditing can enable timely detection of harmful behavior in a system by testing, evaluating, analyzing vulnerabilities, and tracking violations. Pang and Tanriverdi (2022) stated threat actors attempt to capitalize on weak points and vulnerable systems leading to security breaches. When IT security

professionals perform routine security auditing, they are more likely to identify gaps or new risks within their network. According to Al-Matari et al. (2021), security auditing is seen as a constant defense, offense, approach to overall network security. Thus, the IT security professional must adjust their policies and procedures to reduce or eliminate risk as new threats and gaps become known.

One successful approach to security auditing is constantly auditing and looking for weakness in systems. According to Bonaci et al. (2022), as new security risk emerges, there must be an equal response to off-set them by new technologies and procedures. P3 stated, from a project and initiative perspective, making sure security has a seat at the table really helps to integrate security awareness across the enterprise. According to Huang and Liu (2022), attackers are looking for vulnerabilities as these are the entry points to a system. Asset owners need to identify these weaknesses and assess the security implications that can arise from the weakness in a system, essentially thinking like an attacker. One essential way to do achieve this is by conducting penetration testing routinely. Ghanem and Chen (2020) stated penetration testing is a proactive method for evaluating systems and their vulnerabilities, emulating the steps an attacker would take in a real-world scenario.

The theme for security auditing is in alignment with the TAM, which served as the conceptual framework for this study. According to Luo et al. (2020), internal employees represent some of the largest threats when it comes to an organization's information security, as they have inside access to the organization's assets and information. Thus, auditing employee access and activity is vital in disrupting an insider

malicious breach. The TAM framework is used to look at systems use and acceptance through the lens of the employee based on perceived usefulness and ease of use. According to Nasirpouri et al. (2022), when employees see a system that is valuable in assisting their role, they are more willing to utilize the system in the manner that it is deemed for. Additionally, if user does not accept a system as useful or easy to use, the employee may attempt to use a system in a manner not in accordance with the organizations information security policy. Ahmad et al. (2019) stated auditing user activity and procedures verifies how and when a user is accessing systems and the resources that reside on those systems.

According to Arbanas et al. (2021), technical measures should be properly and consistently used by individuals, and depending on individual behavior, can strengthen or weaken security for an organization. P1 stated when bringing on new systems, at least one manager from a few different departments is brought in to test the system. Sometimes a manager will designate key staff to be testers of the new system and the staff will test things as the system goes through the implementation process.

Based on the finding of this study, security auditing is used by IT security professionals to focus on reviewing or adjusting policies and procedures to strengthen the overall security posture of the organization. To accomplish this, IT security professionals must evaluate not only systems, but the user process and behavior toward policies and procedures in relation to systems. Which encompasses the key concepts of the TAM.

Theme 3: Technology Adaptive

The third major theme discovered during data analysis phase of my study involved adaptability. Technology adaptability theme consists of how an organization adapts to changes in their environment and technology improvements. The landscape of IT is ever evolving with new technology and trends that change how an organization may conduct business. This was seen in the COVID-19 pandemic where organizations were forced to adapt to a situation that left many workers without the ability to come into a traditional brick and mortar building. The ability to adapt to technology and environments is critical to an organization for continuing to operate. When done effectively, the strategies implemented for proper security practices in a small financial institution to prevent security breaches. Table 3 below shows the frequency in which the theme was drawn.

Table 3

References for Technology Adaptive

	Participant	
Major Theme	Count	References
Technology Adaptive	3	28

All the participants noted their organizations most recent adaptive situation involved dealing with COVID-19 and employing a wider remote work initiative. When dealing with technology adaptive situations, an organization will have to revisit their policies and procedures to see where new technology fits in accordance with current security for the organization. In the COVID-19 situation, this meant looking at how to provide employees a way to connect to the organization without physically being in the

office, but still allow them to function as if they were. P2 stated during the pandemic they had to deal with remote work which included training individuals, verifying security was in place, then double checking the security was configured correctly through device management and multi-factor authentication. Remote work isn't something new to organizations and in the past has typically been implemented for limited users on a need only basis.

Staying abreast to new technology is beneficial in improving business efficiencies and growing an organization. P3 stated they want to leverage technology to help meet strategic goals of the organization. However, new technology is not always successful due to different factors such as, inefficient resources to implement and manage new technologies, or low acceptance rate causing the organization to abandon the push of a new technology or process.

Adoption rate of new technologies for an organization can be a deciding factor for success or failure when adapting a new process or technology. P2 noted they take user feedback into consideration and try to understand their position and then will go from there. P3 discussed the use of password managers and the resistance the users had toward adapting the technology, this led P3 and their organization to look for alternative solutions such as, biometrics. Sometimes the deciding factor on a technology is resources available to manage the new processes and procedures. P1 noted most small financial institutions need people that can wear multiple hats for different technologies.

Being technology adaptive means consistently looking for new technologies to overcome challenges, according to Mosteanu (2020), but also comes with new additional

risks such as cyberattacks. Finding ways to reduce the risk and improve the efficiencies of the organization allows for a consistent sustainability and even potential growth. P3 noted they like to present strategically when it comes to technology. For example, here is what our clients are trying to do. How can we create the opportunities for them that are secure and available?

The next section of my study focused on correlating the theme of adaptive technology to existing and recent literature. According to Kaur and Sharma (2020), VPN networks create an encrypted channel over a public network to ensure the communication of data is kept confidential. VPN can provide an easy solution for organizations when implementing remote work. Furthermore, instituting MFA, the process of combining different forms of authentication to prove the user is whom they claim to be (Sain et al., 2021). Combining MFA with VPN can decrease the likelihood of a threat actor using an employee credentials to gain access through the VPN. As noted by all the participants, during the COVID-19 pandemic, each organization adapted to allowing employees to work remotely utilizing VPN connections and instituting MFA to further strengthen security for remote work.

More recent literature further supports the theme for adaptive technology as a strategy for proper security practices for small financial institutions to prevent security breaches. According to Mark et al. (2022), the COVID-19 pandemic forced organizations to develop strategies for individuals to rapidly switch from office to home, with these changes predicted to last after the pandemic. P3 noted where remote work has become a way of doing business and they plan to continue conducting remote work for the

foreseeable future. A recent study by Tiwari and Raman (2022), suggests that in the IT industry successful leaders need to possess the ability to change, adopt, and integrate technology. This requires IT security professionals to staying abreast of new technology and test how these technologies can better assist their organization. As suggested by P1, that IT security professionals need to be knowledgeable, able to communicate, and assimilate how technology fits into their environment.

The next section I discuss how adaptive technology theme supports the conceptual framework TAM which I used for this study. According to Sinha and Mukherjee (2016), the TAM attempts to address the process of acceptance of the technology and the usage by consumers of that technology. P3 noted security is not happening in a vacuum where we're reliant on people and so influence is very important; it's the currency we have. IT security professionals are faced with difficult tasks of securing a network in such a way to prevent security breaches, but also easy enough for users to still be able to function. By communicating the reasons for secure process and procedures, IT security professionals can have a positive affect on the behavior a user has toward a system. P2 stated sometimes they get a little push back from managers, but we just explain why the procedure is set the specific way and then everything seems to work out. According to Stylios et al. (2022), TAM is a simple model consisting of fundamental components that explain technology acceptance. When an IT security professional uses the lens of TAM to evaluate how a technology is used from a non-technical perspective, the IT security professional can adjust their processes more effectively, potentially increasing the acceptance rate of a technology. Each participant noted taking user

feedback into account, but ultimately the goal for IT security professionals is to secure the organization from data breaches. Senior management has the final verdict on enforced policy and procedures, and it is up to the IT security professional to ensure those policies are complacent with technology used by the organization.

Theme 4: Vendor Relationships

The fourth and final theme I found within the thematic analysis was vendor relationships. Vendor relationships are vital for an organization as they offer products and services a business needs to perform their business functions. In this study of strategies for proper security practices for small financial institutions to prevent data breaches, vendor relationship consists of two forms: third party vendors and cloud technology vendor relationships. Schneckenberg et al. (2021) stated cloud technology is an integrated digital infrastructure that can combine various technologies. According to Saini et al. (2022), cloud service providers focus on security mechanisms primarily, as data security must consistently be reviewed and adjusted to address and anticipate future attacks. Table 4 below shows the frequency in which the vendor relationship theme was drawn.

Table 4

References to Vendor Relationships

	Participant	
Major Theme	Count	References
Vendor Relationships	3	26

Each participant discussed using vendors to accomplish an overall secure posture for their organization. According to Alexandrova (2015), the role of partnerships has increased and has become a critical resource for organizations. This requires

organizations to assess vendors and identify high risk vendors, that if impacted, would cause major disruptions to an organization's daily operations. P1 noted how the work for managing vendors was different than managing on premises environments. In cloud-based solutions, there is more checking up on vendor management, reviewing service level agreements are being met, working with vendors to ensure due diligence and due care has taken place.

Critical vendors often have direct access to an organizations network, typically through a VPN connection, which provides an open connection from the vendor to the organization. This becomes a security concern if a vendor experiences a security breach, the threat actor may have an open channel to breach the organization as well. P3 stated how connections from vendors are disabled by default and vendors are also not allowed to bring their own equipment on site when visiting. If a vendor needs access to the company network, we provide a workstation, which allows us to log and monitor everything the vendor is doing. Thus, removing the security risk that if a vendor equipment contains malware, it doesn't allow the malware access to the customers network.

The next section of the study I tied the theme to the existing literature as well as to recent literature. Cleary and Mclarney (2019) stated when a business introduce a third-party product, vendor, or application into their organization, vendor management of that system should be established. Vendors that provide critical products for organizations daily functions often maintain a remote connection for troubleshooting a product to ensure mission critical operations. One of the most common ways for this is through

VPNS. The use of VPNS from vendors to organizations may also be used for daily functions such as the need for information to be securely transferred between vendor and organizations. According to Ndichu et al. (2020), VPNS pose a risk to an organization as VPNs evade firewalls and IDS by encrypting all the traffic traversed between the connected devices. This introduces a security vector for threat actors to exploit if the vendor network becomes breached. Allowing the threat actors to span from vendor to additional organizations.

As noted by all participants, their cloud solutions are incorporated into their business processes, which means the data no longer resides within the organizations storage network but is stored and retained on the vendor's infrastructure. One of the most efficient ways to secure the data when it is not being used is by encrypting the data at rest. This means using a cryptography algorithm to hide the true contents of the data until the data is to be used. For a business to understand what preventative measures they need to take to secure their data, they need to answer questions regarding the data they plan to retain. Matloob and Siddiqui (2017) stated the risk questions may include: Who has access to our data; Where, when, and how is our data being accessed; What type of data are we storing; What means is our data being accessed through? Evaluating vendor service level agreements (SLA), contract obligations, and standard procedures answers these questions to ensure data is secure in the cloud as it is on premise within the organization.

In recent literature, Campbell (2018) stated vendor control has typically been accomplished by access control. Where the vendors ability to connect is controlled and

their activity is recorded. This allows the IT security professional to review access and track activity through logging. All generated logs typically comprise of four things: the activity that took place, the process instance, the resource used, and the time at which the event occurred (Chiu & Jans, 2019). P2 stated when a vendor is granted access into a system, it is all tracked and logged for review. According to Yeboah-Ofori et al. (2021), controls are the security mechanisms for an organization to secure their operations and processes. This involves the use of various controls such as detective control like firewalls, IPS, IDS and preventive controls such as policy and procedures. Furthermore, Aparajit et al. (2022) stated organizational policy, monitoring and logging, are techniques for keeping data secure. When an organization applies these strategies toward vendor management, the organizations can limit the exposure of their data to vendors.

The next section I discussed how the vendor relationship theme supports the conceptual framework TAM which I used for this study. According to Ram and Selvabaskar (2022), the TAM is user-centric, and focuses on mapping BI for acceptance of a technology. Organizations do not always have resources to build solutions or products themselves, and therefore seek solutions offered by vendors and third parties. Furthermore, Kumar et al. (2021) stated TAM considers two variables, PEOU and PU. Organizations when choosing a solution offered by a vendor will test the product first. Testing involves seeing how easy the solution is to manage, and if the solution is effective in meeting the organization's business need. P2 stated when searching for a security solution, we tested different vendors but a lot of them just didn't work for our organization. Furthermore, P2 explained the usefulness of one vendor by assisting them

in strengthening their overall security posture. Organizations evaluate vendors based on their products offered and form a relationship if they see value for the products in how they can assist an organization achieve their overall objectives.

The themes I identified in this study align with current research and illustrate an effective IT security posture must align with current trends, technologies, and the overall objectives of an organization. The strategies I discussed in this study correlate with existing literature and can be integrated with the TAM, which I used as the conceptual framework for this study.

Applications to Professional Practice

The findings I discovered in this study resulted in some key themes and various strategies that IT security professionals are currently employing to achieve a strong security posture within their institution. By exploring these strategies other IT security professionals may adopt the strategies or use the strategies to form tailored strategies of their own to protect an institution from security breaches. According to Liu (2021), a magnitude of data breaches from cybersecurity attacks on financial institutions is frequently associated with ineffective security practices and procedures. The findings I discussed in this study may benefit IT security professionals by providing them examples of strategies I discovered in this study that if adopted, may close gaps within their current security strategies.

Implications for Social Change

The findings I discovered in this study advocate that there can be improvements to the strategies used by IT security professionals for implementing proper security

practices in small financial institutions to prevent security breaches. According to Huaman et al. (2022), the changes in technologies are shifting business processes, the data and information of customers is an important asset requiring appropriate levels of security and control. By applying proper strategies to prevent security breaches, the organizations are protecting customer data and information from threat actors looking to steal customers information for personal gain. Additionally, security breaches can have an overall negative affect on an organization. Demjaha et al. (2019) stated post security breach, employees are often sanctioned to re-read security policies and forced to comply with new governed policies. This can lead to disgruntled employees causing further security issues. In the end, customers as well as employees of financial institutions will benefit knowing the organization is proactively pursuing secure measures to safeguard data from threat actors.

Recommendations for Action

The findings I discovered in this study could benefit IT security professionals around the world by providing IT security professionals with strategies they could implement related to proper security practices. The first recommendation I suggest is for IT security professionals to review existing layered security that is currently in place to prevent security breaches and determine if they align with the ones I presented in this study. Additionally, IT security professionals should review existing security appliances and compare them to available products in the market. By doing an existing technology review, IT security professionals may identify if current security appliances can be improved by replacing existing equipment with newer technology to strengthen overall

security posture. Furthermore, any organization operating without a strategy for layered security should review this study and determine if one of the strategies I uncovered in this study could work for their institution.

The second recommendation I suggest is for IT security professionals to review existing security auditing practices and compare them with ones presented in this study. Security auditing provides insight to what is occurring on an institutions system daily. By actively reviewing the organizations auditing practices, an IT security professional can adapt their procedures to current security trends, further strengthening the ability to prevent security breaches. Furthermore, IT security professionals should review how they're staying up to date on current security trends to ensure they are being informed about the latest security threats and how to offsite threats within their organization.

The third recommendation I suggest is for IT security professionals to perform a review of existing procedures and policies for unforeseen events in the future. IT security professionals should examine current system processes to determine how to continue those daily functions in unforeseen circumstances. By doing this, IT security professionals will be better prepared for dealing with future events without having to compromise security, potentially leading to a security breach. Any organization that currently doesn't have strategies for being technology adaptive should review this study and determine if one of the strategies I uncovered in this study can provide them guidance.

The last recommendation for action I suggest is for an organization to conduct a review of existing vendors and the relationship dependency for that vendor.

Organizations use vendors for a variety of services and should be cognizance of their critical vendors and the services they provide. Organizations should review auditing practices for visibility on tracking vendor access within the organization's infrastructure. Any organization that currently doesn't have strategies for vendor management should review my study and see if one of the strategies I uncovered in this study may be adopted into their organization to limit vendor access. Furthermore, IT security professionals should identify vendor's policies and practices to verify the third party is applying proper security on their systems to reduce the risk of security breaches.

Regarding dissemination, I provided a strategy summary for proper security practices for small financial institutions to participants through e-mail. This provided them a summary of my findings and recommendations so that the participants themselves my benefit from the findings of my study. Additionally, by providing the participants a copy of my study, each participant can distribute the summary of my findings to other institutions for continued referencing. Lastly, my study will be available in the ProQuest database for future scholars to reference. I also plan to submit my study to other academic journals, especially journals that focus on credit unions. My goal is to make my study available so that small financial institutions can reference my study when implementing strategies for proper security practices within their financial institution to prevent security breaches.

Recommendations for Further Study

Security is a continuous journal that must be reviewed and adjusted as new threats and technology become available. My study provided strategies IT security professionals

are currently using for proper security practices to prevent security breaches. However, as security changes, new threats are discovered. The financial sector is one of the top sectors cyber criminals target due to the sensitive data that is stored within financial institutions. Further studies may benefit financial institutions as the threat landscapes continue to evolve, future studies may provide new strategies for the emerging threats.

The limitations of this study were primarily my sample size and documentation available for triangulation. I recommend that researchers expand the sample size to include larger financial institutions. This will increase the geographical size of any future study which will increase the sample size. Furthermore, I recommend studying target focused processes within financial institutions. My study provided a wide range of strategies for proper security practices to prevent security breaches. Limited documentation was able to be provided to ensure security was maintained for each organization. A further study may narrow the focus to a specific strategy to obtain organization documentation assisting in triangulation.

Reflections

My study was a great endeavor for me personally. As the researcher, I tried to be cognizance of any bias when recording data to ensure my study remained credible. I was the primary instrument for recording and analyzing the data, so being aware of my bias and strictly focusing on the recorded responses ensured I alleviated bias within my study. Throughout the interviews, I followed a standard protocol of questions. I performed member checking with each participant to ensure my recorded responses were accurate.

Since one of my limitations was obtaining internal documents, I reviewed publicly available NIST documents to complete triangulation.

Over the course of my study, I have learned new strategies for proper security practices. I also learned about how organizations handled the COVID-19 pandemic and were successful in changing the process in which individuals now work; even after the pandemic has subsided. Lastly, I learned how each organization may use different technology to achieve the same goal, which shows there is more than one way to perform successful strategies for proper security practices.

Summary and Study Conclusions

The purpose of my study was to explore strategies used by IT security professional for proper security practices in small financial institutions to prevent security breaches. The qualitative multi-case study used TAM for the conceptual framework and methodological triangulation which consisted of recorded interviews, member-checking, and reviewing publicly accessible documentation. The four key themes I discovered in the study findings were: layered security, security auditing, technology adaptive, and vendor relationships. The data I uncovered in this study when combined can provide financial institutions strategies to prevent security breaches. Lastly the findings of my study may contribute to social change because they may be beneficial to other IT security professionals in creating strategies to safeguard their institutions from security breaches and keeping the institutions' customers data out of threat actors' hands.

References

Abbas, H. (2016). Subjective norm as antecedents of consumers' behavioral intentions to use smart phones in arab world. *Journal of Mobile Technologies, Knowledge and Society*, *2016*(2016). https://doi.org/10.5171/2016.863777

Abdalla, M. M., Oliveira, L. G., Azevedo, C. E., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulation as a methodological alternative. *Administração: ensino e pesquisa, 19*(1), 66–98. https://doi.org/10.13058/raep.2018.v19n1.578

Abdulghani, H. A., Nijdam, N. A., Collen, A., & Konstantas, D. (2019). A study on security and privacy guidelines, countermeasures,threats: IoT data at rest perspective. *Symmetry*, *11*(6) 774. https://doi.org/10.3390/sym11060774

Aborisade, O. P. (2013). Data collection and new technology. *International Journal of Emerging Technologies in Learning, 8*(2), 48–52. https://doi.org/10.3991/ijet.v8i2.2157

Abu Othman, N. A., Norman, A. A., & Mat Kiah, M. L. (2021). Information system audit for mobile device security assessment. *2021 3rd International Cyber Resilience Conference (CRC)*. https://doi.org/10.1109/crc50527.2021.9392468

Adhabi, E., & Anozie, C. (2017). Literature review for the type of interview in qualitative research. *International Journal of Education, 9*(3), 86–97. https://doi.org/10.5296/ije.v9i3.11483

Ahmad, A., Saad, M., & Mohaisen, A. (2019). Secure and transparent audit logs with blockaudit. *Journal of Network and Computer Applications, 145*(1).

https://doi.org/10.1016/j.jnca.2019.102406

Ahmad, M. (2018). Review of the technology acceptance model (TAM) in internet banking and mobile banking. *International Journal of Information Communication Technology and Digital Convergence, 3*(1), 23–41. https://tinyurl.com/maenadv9

Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin, 84*(5), 888–918. https://doi.org/10.1037/0033-2909.84.5.888

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Prentice-Hall.

Ajzen, I., & Madden, T. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology, 22*(5), 453–474. https://doi.org/10.1016/0022-1031(86)90045-4

Akhawe, D., Amann, B., Vallentin, M., & Sommer, R. (2013). Here's my cert, so trust me, maybe? *Proceedings of the 22nd International Conference on World Wide Web*, https://doi.org/10.1145/2488388.2488395

Akinyode, B., & Khan, T. (2018). Step by step approach for qualitative data analysis. *International journal of Built Environment and Sustainability*, *5*(3), 163–174. https://doi.org/10.11113/ijbes.v5.n3.267

Alassaf, M., & Alkhalifah, A. (2021). Exploring the influence of direct and indirect factors on information security policy compliance: A systematic literature review. *IEEE Access, 9*, 162687–162705. https://doi.org/10.1109/access.2021.3132574

Aldiabat, K., & Le Navenec, C. (2018). Data saturation: the mysterious step in grounded theory methodology. *The Qualitative Report, 23*(1), 245–261. https://tinyurl.com/5fkvf39r

Alexandrova, M. (2015). Risk factors in IT outsourcing partnerships: vendors' perspective. *Global Business Review, 16*(5), 737–906. https://doi.org/10.1177/0972150915591427

Almasri, B. M., & McDonald, D. D. (2021). Philosophical assumptions used in research on barriers for effective cancer pain management: a scoping review. *Pain Management Nursing, 22*(5), 634–644. https://doi.org/10.1016/j.pmn.2021.04.006

Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2021). Adopting security maturity model to the organization's capability model. *Egyptian Infomatics Journal, 22*(2), 193–199. https://doi.org/10.1016/j.eij.2020.08.001

Almeida, F. (2018). Strategies to perform a mixed methods study. *European Journal of Education Studies, 5*(1), 137–151. http://dx.doi.org/10.46827/ejes.v0i0.1902

ALSaleem, B. O., & Alshoshan, A. I. (2021). Multi-factor authentication to systems login. *2021 National Computing Colleges Conference (NCCC).* https://doi.org/10.1109/NCCC49330.2021.9428806

Alvarez, J., Zamora, Y., Pina, I., & Angarita, E. (2021). Demilitarized network to secure the data stored in industrial networks. *International Journal of Electrical and Computing Engineering*, 611–619. https://doi.org/10.11591/ijece.v11i1

Amin, M. E., Nørgaard, L. S., Cavaco, A. M., Witry, M. J., Hillman, L., Cernasev, A., & Desselle, S. P. (2020). Establishing trustworthiness and authenticity in qualitative

pharmacy research. *Research in Social and Administrative Pharmacy, 16*(10), 1472–1482. https://doi.org/10.1016/j.sapharm.2020.02.005

Aminzade, M. (2018). Confidentiality, integrity and availability- finding a balanced IT framework. *Network Security 2018*(5), 9–11. https://doi.org/10.1016/S1353-4858(18)30043-6

Andress, J. (2014). *The Basics of Information Security.* Syngress.

Anna, K. O. (2020). Methods of security authentication and authorization into informationals systems. *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*. https://doi.org/10.1109/ATIT50783.2020.9349333

Aparajit, S., Shah, R., Chopdekar, R., & Patil, R. (2022). Data protection: The cloud security perspective. *2022 3rd International Conference for Emerging Technology*. https://doi.org/10.1109/INCET54531.2022.9825151

Arbanas, K., Spremic, M., & Zajdela Hrustek, N. (2021). Holistic framework for evaluating and improving information security culture. *Aslib Journal of Information Management, 73*(5), 699–716. https://doi.org/10.1108/AJIM-02-2021-0037

Archer, E. (2018). Qualitative data analysis: A primer on core approaches. *Online Readings in Research Methods*, 1–23. https://tinyurl.com/5eptp364

Arenas-Gaitan, J., Ramirez-Correa, P., & Rondan-Cataluna, F. (2015). A comparison of the different versions of popular technology acceptance models: A non-linear perspective. *The international journal of cybernectices, systems and management*

services, 44(5), 788–805. https://doi.org/10.1108/K-09-2014-0184

Arifin, S. R. (2018). Ethical considerations in qualitative study. *International Journal of Care Scholars, 1*(2), 30–33. https://doi.org/10.31436/ijcs.v1i2.82

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

Ballena, C. (2021). Qualitative research interviewing: typology of graduate students' interview questions. *Philippine Social Science Journal, 4*(3), 96–112. https://tinyurl.com/mstjwwbs

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist, 37*(2), 122–147. https://doi.org/10.1037/0003-066X.37.2.122

Barabanov, A., & Makrushin, D. (2021). Security audit logging in microservice-based systems: Survey of architecture patterns. *Network Security*, 71–80. https://doi.org/10.21681/2311-3456-2021-2-71-80

Barrett, D., & Twycross, A. (2018). Data collection in qualitative research. *Evidence-Based Nursing, 21*, 63–64. http://dx.doi.org/10.1136/eb-2018-102939

Batool, H., & Masood, A. (2020). Enterprise mobile device management requirements and features. *IEEE Conference on Computer Communications Workshops*. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162763

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

Bayuk, J., & Silverstein, K. (2007). Utilising information security to improve resilience. *Journal of Business Continuity & Emergency Planning, 2*(1), 7–12.

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

Benqdara, S., Sultan, A., & Elfergani, A. (2018). Building security perimeters to protect banking sector in libyan. *International Journal of Computer Applications*, 975, 8887. https://tinyurl.com/ybtzkcsz

Bergen, N., & Labonte, R. (2020). "Everything is perfect, and we have no problems": detecting and limiting social desirability bias in qualitative research. *Qualitative Health Research, 30*(5), 783–792. https://doi.org/10.1177/1049732319889354

Bernard, R. (2012). *Social research methods: Qualitative and quantitative approaches.* Sage.

Berndt, A. (2020). Sampling methods. *Journal of Human Lactation, 36*(2), 224–226. https://doi.org/10.1177/0890334420906850

Bhattacherjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly, 25*(3), 351–370. https://doi.org/10.2307/3250921

Bonaci, T., Michael, K., Rivas, R., Robertson, L. J., & Zimer, M. (2022). Emerging technologies, evolving threats: next-generation security challenges. *IEEE Transactions on Technology and Society*. https://doi.org/10.1109/TTS.2022.3202323

Brantlinger, E., Jimenez, R., Klingner, J., Pugach, M., & Richardson, V. (2005). Qualtitative studies in special education. *Exceptional children, 71*(2), 195–207. https://doi.org/10.1177/001440290507100205

Brobst, J., & Council, C. (2005). Using IT governance. *Community College Journal*, *76*(2) 30.

Byrne, D. (2021). A worked example of braun and clarke's approach to reflexive thematic analysis. *Quality & Quantity*, *56*(3), 1–21. https://doi.org/10.1007/s11135-021-01182-y

Campbell, C. (2018). Securing the vendor: changing the dynamic of the infosec relationship. *ISSA Journal, 16*(1), 37–40.

Candela, A. (2019). Exploring the function of member checking. *The Qualitative Report, 24*(3), 619–628.

Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. *2017 IEEE International Conference on Big Data (Big Data),* https://doi.org/10.1109/BigData.2017.8258485

Chiu, T., & Jans, M. (2019). Process mining of event logs: a case study evaluating internal control effectiveness. *Accounting Horizons*, 141–156. https://doi.org/10.2308/acch-52458

Chowdhary, A., Huang, D., Mahendra, J., Romo, D., Deng, Y., & Sabur, A. (2020). Autonomous security analysis and penetration testing. *2020 16th International Conference on Mobility, Sensing and Networking (MSN)*. https://doi.org/10.1109/MSN50589.2020.00086

Clark, K., & Veale, B. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology, 89*(5), 482CT–485CT.

Cleary, S., & Mclarney, C. (2019). Organizational benefits of an effective vendor management strategy. *Journal of Supply Chain Management*, 50–67.

Coffelt, T. (2017). *Confidentiality and anonymity of participants.* The SAGE Encyclopedia of Communication Research Method.

Cook, D., Giacomini, M., & Sinuff, T. (2007). How qualitative research can contribute to research in the intensive care unit. *Journal of Critical Care, 22*(2), 104–111. https://doi.org/10.1016/j.jcrc.2007.03.001

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

Cyriac, N., & Sadath, L. (2019). Is cyber security enough- a study on big data security breaches in financial institutions. *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*. https://doi.org/10.1109/ISCON47742.2019.9036294

Dash, M., Mohanty, A., Pattnaik, S., & Sahoo, S. (2011). Using the TAM model to explain how attitudes determine adoption of internet banking. *European Journal of Economics, Finance, and Administrative Sciences*(36), 51–59. https://tinyurl.com/bdemk5jk

Davis, F. (1985). *A technology acceptance model for empirically testing new end-user*

information systems: theory and results (Doctoral dissertation, Massachusetts Institute of Technology). https://tinyurl.com/bdhznffh

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

de Cassia Nascimento, L., Vignuda de Souza, T., Oliveria, I. C. dos S., de Montenegro Medeiros de Moraes, J. R., Cordeiro Burla de Aguiar, R., & Faria da Silva, L. (2018). Theoretical saturation in qualitative research: An experience report in interview with schoolchildren. *Revista Brasileira de Enfermagem*, *71*(1) 228–233. https://doi.org/10.1590/0034-7167-2016-0616

DeJonckheere, M., & Vaughn, L. (2019). Semistructured interviewing in primary care research: A balance of relationship and rigour. *Family Medicine and Community Health, 7*(2). https://doi.org/10.1136/fmch-2018-000057

Demjaha, A., Caulfield, T., Angela Sasse, M., & Pym, D. (2019). 2 fast 2 secure: A case study of post-breach security changes. *2019 IEEE European Symposium on Security and Privacy Workshops*. https://doi.org/10.1109/EuroSPW.2019.00028

Diefenbach, T. (2009). Are case studies more than sophisticated storytelling?: Methodological problems of qualitative empirical research mainly based on semi-structed interviews. *Quality and Quantity, 43*(6), 875–894. https://doi.org/10.1007/s11135-008-9164-0

Dishaw, M. T., & Strong, M. (1999). Extending the technology acceptance model with task-technology fit constructs. *Information & Management*, *36*(1), 9–21.

https://doi.org/10.1016/s0378-7206(98)00101-3

Djerouni, M. (2019). Implication of Employees in Security Policies Definition. *International Journal of Information Security & Cybercrime, 8*(1), 23–29. https://doi.org/10.1016/S0378-7206(98)00101-3

Dzwigol, H. (2020). Methodlogical and Empirical platform of triangulation in strategic management. *Academy of Strategic Management Journal, 19*(4), 1–8.

Eldh, A., Arestedt, L., & Bertero, C. (2020). Quotations in qualitative studies: reflections on constituents, custom, and purpose. *International Journal of Qualitative Methods, 19*, 1–6. https://doi.org/10.1177/1609406920969268

Ellis, P. (2020). Sampling in qualitative research (1). *Wounds UK*, *16*(3) 82–83.

El-Temtamy, O., Majdalawieh, M., & Pumphrey, L. (2016). Assessing IT disaster recovery plans: the case of publicly listed firms on Abu Dhabi/UAE security exchange. *Information & Computer Security, 24*(5), 514–533. https://doi.org/10.1108/ICS-04-2016-0030

Etikan, I., & Bala, K. (2017). Sampling and sampling methods. *Biometrics & Biostatistics International Journal, 5*(6), 149. https://doi.org/10.15406/bbij.2017.05.00149

Fay, J., & Patterson, D. (2018). *Contemporary Security Management.* Butterworth-Heinemann.

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

FitzPartick, B. (2019). Validity in qualitative health education research. *Currents in*

Pharmacy Teaching and Learning, 11, 211–217. https://doi.org/10.1016/j.cptl.2018.11.014

Fockel, M., Merschjohann, S., & Fazal-Baqaie, M. (2018). Threat analysis in practice - systematically deriving security requirements. *Conference: 19th International Conference on Product-Focused Software Process Improvement.* https://doi.org/10.1007/978-3-030-03673-7_25

Forte, D., & Power, R. (2007). Physical security – overlook it at your own peril. *Computer Fraud & Security*, *2007*(8) 16–20. https://doi.org/10.1016/S1361-3723(07)70105-7

Furnell, S. (2016). Vulnerability management: Not a patch on where we should be? *Network Security*, *2016*(4) 1–5. https://doi.org/10.1016/S1353-4858(16)30036-8

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security, 100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

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

Ghanem, M. C., & Chen, T. M. (2020). Reinforcement learning for efficient network penetration testing. *Information (2078-2489), 11*(1), 6. https://doi.org/10.3390/info11010006

Gill, S. (2020). Qualitative sampling methods. *Journal of Human Lactation, 36*(4), 579–581. https://doi.org/10.1177/0890334420949218

Goshwe, N. (2013). Data encryption and decryption using RSA algorithm in a network

environment. *International Journal of Computer Science and Network Security*, *13*(7) 9–13 . https://www.academia.edu/download/52104438/20130702.pdf

Goulding, C. (2005). Grounded theory, ethnography and phenomenolgy: A comparative analysis for three qualitative strategies for marketing research. *European journal of Marketing, 39*(3/4), 294–308. https://doi.org/10.1108/03090560510581782

Green, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. *Educational evaluation and policy analysis, 11*(3), 255–274. https://doi.org/10.3102/01623737011003255

Guetterman, T., & Fetters, M. (2018). Two methodological approaches to the integration of mixed methods and case study designs: A systematic review. *American Behavioral Scientist, 62*(7), 900–918. https://doi.org/10.1177/0002764218772641

Hamoud, A., & Aimeur, E. (2020). Handling user-oriented cyber-attacks: STRIM, a user-based security training model. *Computer Science*, *2*. https://doi.org/10.3389/fcomp.2020.00025

Hanif, Y., & Lallie, S. H. (2021, November). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM - with perceived cyber security, risk, and trust. *Technology in Society, 67*, 101693. https://doi.org/10.1016/j.techsoc.2021.101693

Harryanto, Muchran, M., & Ahmar, A. S. (2018). Application of tam model to the use of information technology. *International Journal of Engineering & Technology (UAE), 7*(2.9), 37–40. https://doi.org/10.48550/arXiv.1901.11358

Haven, T., & Grootel, L. (2019). Preregistering qualitative research. *Accountability in Research, 26*(3), 229–224. https://doi.org/10.1080/08989621.2019.1580147

Hayashi, P., Abib, G., & Hoppen, N. (2019). Validity in qualitative research: A processual approach. *The Qualitative Report, 24*(1), 98–112. https://doi.org/10.46743/2160-3715/2019.3443

Heath, J., Harcourt, D., Williams, H., & Williams, L. (2018). "It's just more personal": using multiple methods of qualitative data collection to facilitate participation in research focusing on sensitive subjects. *Applied Nursing Research, 43*, 30–35. https://doi.org/10.1016/j.apnr.2018.06.015

Herzog, C., Handke, C., & Hitters, E. (2019). Analyzing talk and text II: thematic analysis. In: Van den Bulck, H., Puppis, M., Donders, K., Van Audenhove, L. (eds) *The Palgrave Handbook of Methods for Media Policy Research* (pp. 385–401). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-16065-4_22

Hong, Y., & Funell, S. (2019). Organizational formalization and employee information security behavioral intentions based on an extended TPB model. *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. https://doi.org/10.1109/CyberSecPODS.2019.8885405

Hooper, V., & Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology, 39*(8), 862–874. https://doi.org/10.1080/0144929X.2019.1623322

Hossain, M. J. (2021). ICAS: two-factor identity-concealed authentication scheme for remote-servers. *Journal of Systems Architecture*, *117*, 102077.

https://doi.org/10.1016/j.sysarc.2021.102077

Howard, M., & Rose, J. (2018). Refining and extending task-technology fit theory: Creation of two task-technology fit scales and empirical clarification of the construct. *Information & Management*, *56*(6), 103134. https://doi.org/10.1016/j.im.2018.12.002

Hsieh, G., & Kocielnik, R. (2016). You get who you pay for: The impact of incentives on participation bias. *In Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing*. https://doi.org/10.1145/2818048.2819936

Hu, P. (2020). Computer testing and maintenance and data recovery technology. *Journal of Physics: Conference Series, 1648*(2), 022198. https://10.1088/1742-6596/1648/2/022198

Hu, Z., Ding, S., Li, S., Chen, L., & Yang, S. (2019). Adoption intention of fintech services for bank users: an empirical examination with an extended technology acceptance model. *Symmetry, 11*(3), 340. https://doi.org/10.3390/sym11030340

Huaman, C. H., Fuster, N. F., Luyo, A. C., & Armas-Aguirre, J. (2022). Critical data security model: Gap security identification and risk analysis in financial sector. *17th Iberian Conference on Information Systems and Technologies*. https://10.23919/CISTI54924.2022.9820547

Huang, B., & Liu, Y. (2022). A network vulnerability assessment method using general attack tree. *5th International Conference on Data Science and Information Technology*. https://doi.org/10.1109/DSIT55514.2022.9943814

Irani, E. (2019). The use of videoconferencing for qualitative interviewing: opportunities, challenges, and considerations. *Clinical Nursing Research,* 28(1), 3–8. https://doi.org/10.1177/1054773818803170

Ishlahuddin, A. H. (2020). Analysing IT governance maturity level using COBIT 2019 framework: A case study of small size higher education institute (XYZ-edu). *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE).* https://doi.org/10.1109/IC2IE50715.2020.9274599

Jaber, A., Anwar, S., Khidzir, N., & Anbar, M. (2021). The Importance of IDS and IPS in cloud computing environment: Intensive review and future directions. *Communications in Computer and Informaiton Science, 1347,* 479–491. https://doi.org/10.1007/978-981-33-6835-4_32

Jackson, B. A., & LaTourrette, T. (2015). Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries. *Journal of Air Transport Management, 48*, 26–33. https://doi.org/10.1016/j.jairtraman.2015.06.009

Jacobs, J., Romanosky, S., Adjerid, I., & Baker, W. (2020). Improving vulnerability remediation through better exploit prediction. *Journal of Cybersecurity, 6*(1). https://doi.org/10.1093/cybsec/tyaa015

Jeong, C. Y., Lee, S. Y., & Lim, J. H. (2019). Information security breaches and IT security investments: impacts on competitors. *Information & Management, 56*(5), 681–695. https://doi.org/10.1016/j.im.2018.11.003

Jing Gao, B. Z. (2010). A dynamic authorization model based on security label and role.

2010 IEEE International Conference on Information Theory and Information Security, Information Theory and Information Security (ICITIS). https://doi.org/10.1109/ICITIS.2010.5689504

Jingyao, S., Chandel, S., Yunnan, Y., Jingji, Z., & Zhipeng, Z. (2019). Securing a network: How effective using firewalls and vpns are? *Lecture Notes in Networks and Systems*, 1050–1068. https://doi.org/10.1007/978-3-030-12385-7_71

Johari, R., Kaur, I., Tripathi, R., & Gupta, K. (2020). Penetration testing in IoT network. *2020 5th International Conference On Computing, Communication and Security (ICCCS).* https://doi.org/10.1109/ICCCS49678.2020.9276853

Johnson, J., Adkins, D., & Chauvin, S. (2020). Qualitative research in pharmacy education. *Amercian Journal of Pharmaceutical Edcuation, 84*(1), 138–146. https:www.ajpe.org

Johnson, R. B., & Onwuegbuzie, A. (2004). Mixed methods research: A research paradigm whose time has come. *Educational researcher, 33*(7), 14–26. https://doi.org/10.3102/0013189x033007014

Julianti, M. R. (2021). IT governance framework for academic information system at higher education institutions: a systematic literature review. *2021 International Conference on ICT for Smart Society (ICISS)*. https://doi.org/10.1109/ICISS53185.2021.9533213

Jurn, J., Kim, T., & Kim, H. (2018). An automated vulnerability detection and remediation method for software security. *Sustainability, 10*(5), 1652. https://doi.org/10.3390/su10051652

Kalu, F. A. (2017). What makes qualitative research good research? an exploratory analysis of critical elements. *International Journal of Social Science, 5*(2), 43–56. https://doi.org/10.5296/ijssr.v5i2.10711

Karagiozis, N. (2018). The complexities of the researcher's role in qualitative research: the power of reflexivity. *International Journal of Interdisciplinary Educational Studies, 13*(1), 19–31. https://doi.org/10.18848/2327-011X/CGP/v13i01/19-31

Kaur, C., & Sharma, Y. (2020). The vital role of vpn in making secure connection over internet world. *International Journal of Recent Technology and Engineering*, *8*(6), 2336–2339. https://doi.org/10.35940/ijrte.F8335.038620

Kay, A., Hutcherson, C., Keene, C., Zhang, X., & Terwilliger, M. G. (2021). How financial institutions address cybersecurity threats: a critical analysis. *Issues in Information Systems, 22*(1), 63–74. https://doi.org/10.48009/1_iis_2021_63-74

Kesharwani, A., & Bisht, S. (2012). The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model. *Internation Journal of Banking Marketing, 30*(4), 303–322. https://doi.org/10.1108/02652321211236923

Klein, D. (2021). Relying on firewalls? here's why you'll be hacked. *Network Security*, *2021*(1) 9–12. https://doi.org/10.1016/S1353-4858(21)00007-6

Korovessis, P., Furnell, S., Papadaki, M., & Haskell-Dowland, P. (2017). A toolkit approach to information security awareness and education. *Journal of Cybersecurity Education, Research and Practice*, *2017*(2) 1–31. https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss2/5

Korstjens, I., & Moser, A. (2017). Series: practical guidance to qualitative research. part2: Context, research questions and designs. *European Journal of General Practices, 23*(1), 247–279. https://10.1080/13814788.2017.1375090

Kumar Bhardwaj, A., Garg, A., & Gajpal, Y. (2021). Determinants of blockchain technology adoption in supply chains by small and medium enterprises (SMES) in India. *Mathematical Problems in Engineering*, *2021*, 1–14. https://doi.org/10.1155/2021/5537395

Kumar, M., Meena, J., & Singh, J. (2015). Data outsourcing: A threat to confidentiality, integrity, and availability. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. https://doi.org/10.1109/ICGCIoT.2015.7380703

Laio, C., Palvia, P., & Chen, J.-L. (2009). Information technology adoption behavior life cycle: Toward a technology continuance theory (TCT). *International Journal of Information Management*, *29*(4), 309–320. https://doi.org/10.1016/ijinfomgt.2009.03.004

Lee, Y. H., Hsieh, Y. C., & Hsu, C. N. (2011). Adding innovation diffusion theory to the technology acceptance model: Supporting employees' intentions to use e-learning. *Educational Technology & Society, 14*(4), 124–137.

Lemon, L. & Hayes, J. (2020). Enhancing trustworthiness of qualitative findings: Using leximancer for qualitative data analysis triangulation. *The Qualitative Report, 25*(3), 604–614. https://doi.org/10.46743/2160-3715/2020.4222

Lester, J., Cho, Y., & Lochmiller, C. (2020). Learning to do qualitative data analysis: A

starting point. *Human Resources Development Review, 19*(1), 94–106. https://10.1177/1534484320903890

Liu, X. M. (2021). A risk-based approach to cybersecurity: A case study of financial messaging networks data breaches. *The Coastal Business Journal*, *18*(1), 21–38. https://digitalcommons.coastal.edu/cbj/vol18/iss1/2

Livari, N. (2018). Using member checking in interpretive research practice: A hermeneutic analysis of informants' interpretation of their organizational realities. *Information Technology & People, 31*(1), 111–133 . https://doi.org/10.1108/ITP-07-2016-0168

Luo, X., Li, H., Hu, .., & Xu, H. (2020). Why individual employees commit malicous computer abuse: A routine activity theory perspective. *Journal of the Association for Information Systems, 21*(6), 1552–1593. https://doi.org/10.17705/1jais.00646

Lydia O' Sullivan, L. F. (2021). An evaluation of the process of informed consent: Views from research participants and staff. *Trials, 22*(1), 1–15. https://doi.org/10.1186/s13063-021-05493-1

Mackieson, P., Shlonsky, A., & Connolly, M. (2019). Increasing rigor and reducing bias in qualitative research: A document analysis of parliamentary debates using thematic analysis. *Qualitative Social Work, 18*(6), 965–980. https://doi.org/10.1177/1473325018786996

Maddux, J., & Rogers, R. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Mahmmod, K. F., Azeez, M. M., & Ahmed, M. A. (2020). IPsec cryptography for data packets security within vpn tunneling networks communications. *2020 International Conference on Electrical Engineering and Informatics (ICELTICs)*. https://doi.org/10.1109/ICELTICs50595.2020.9315407

Mark, G., Kun, A. L., Rintel, S., & Sellen, A. (2022). Introduction to this special issue: The future of remote work: Responses to the pandemic. *Human-Computer Interaction, 37*(5), 397–403. https://doi.org/10.1080/07370024.2022.2038170

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualtative research?: A review of qualitative interviews in is research. *Journal of Computer Information Systems, 54*(1), 11–22. https://doi.org/10.1080/08874417.2013.11645667

Martinez, C. V., & Vogel-Heuser, B. (2018). Towards industrial intrusion prevention systems: A concept and implementation for reactive protection. *Applied Sciences-Basel, 8*(12), 2460. https://doi.org/10.3390/app8122460

Matloob, G., & Siddiqui, F. (2017). Data at rest and it's security solutions-a survey. *International Journal of Advanced Research in Computer Science*, *8*(5), 1491–1493.

Matsikidze, H., & Kyobe, M. (2020). A proposed cyber security framework for auditing in financial institutions. *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. https://doi.org/10.1109/IEMCON51383.2020.9284861

McChesney, B. (2006). Aviation security - the convergence of IT and physical security.

IEEE Instrumentation & Measurement Magazine, Instrumentation & Measurement Magazine, 18–20 . https://10.1109/MIM.2006.1634983

McCreight, T., & Leece, D. (2016). Physical security and IT convergence: Managing the cyber-related risks. *Journal of Business Continuity & Emergency Planning*, *10*(1), 18–30.

McGrath, C., Palmgren, P., & Liljedahl, M. (2019). Twelve tips for conducting qualitative research interviews. *Medical Teacher, 41*(9), 1002–1006. https://doi.org/10.1080/0142159X.2018.1497149

McKibbin, K. J., Malin, B. A., & Clayton, E. W. (2021). Protecting research data of publicly revealing participants. *Journal of Law and the Biosciences, 8*(2). https://doi.org/10.1093/jlb/lsab028

Mishra, A. A., Surve, K., Patidar, U., & Rambola, R. K. (2018). Effectiveness of confidentiality, integrity and availability in the security of cloud computing: A review. *2018 4th International Conference on Computing Communication and Automation (ICCCA)*. https://doi.org/10.1109/CCAA.2018.8777537

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Envionment and People, 7*(1), 23–48. https://doi.org/10.26458/jedep.v7il.571

Moser, A., & Korstjens, I. (2018). Series: practical guidance to qualitative research. part 3: Sampling, data collection and analysis. *European Journal of General Practice, 24*(1), 9–18. https://doi.org/10.1080/13814788.2017.1375091

Mosteanu, N. R. (2020). Challenges for organizational structure and design as a result of

digitalization and cybersecurity. *The Business & Management Review, 11*(1), 278–286. https://doi.org/10.24052/bmr/v11nu01/art-29

Mukdasanit, S., & Kantabutra, S. (2021). Attack and defense in the layered cyber-security model and their $(1 \pm \epsilon)$-approximation schemes. *Journal of Computer and System Sciences*, *115*, 54–63. https://doi.org/10.1016/j.jcss.2020.07.001

Munoz-Leiva, F., Climent-Climent, S., & Liebana-Cabanillas, F. (2017). Determinants of intention to use the mobile banking apps: An extension of the classic Tam model. *Spanish Journal of Marketing - ESIC, 21*(1), 25–38. https://doi.org/10.1016/j.sjme.2016.12.001

Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. *Communications of the Association for Information Systems*, *42*, 147–182. https://doi.org/10.17705/1CAIS.04207

Nasirpouri Shadbad, F., & Biros, D. (2022). Technostress and its influence on employee information security policy compliance. *Information Technology & People, 35*(1), 119–141. https://doi.org/10.1108/ITP-09-2020-0610

Nassaji, H. (2020). Good qualitative research. *Language Teaching Research, 24*(4), 427–431. https://doi.org/10.1177/1362168820941288

Ndichu, S., McOyowo, S., Okoyo, H., & Wekesa, C. (2020). A remote access security model based on vulnerability management. *I.J. Information Technology and Computer Science*, *12*(5), 38–51. https://doi.org/10.5815/ijitcs.2020.05.03

Neuendorf, K. (2018). Content analysis and thematic analysis. *Advanced Research*

Methods for Applied Psychology, 211–223. https://doi.org/10.4324/9781315517971-21

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

Pang, M. S., & Tanriverdi, H. (2022). Strategic roles of IT moderization and cloud migration in reducing cybersecurity risks of organizations: The case of US federal government. *The Journal of Strategic Information Systems, 31*(1), 101707. https://doi.org/10.1016/j.jsis.2022.101707

Park, E. (2020). User acceptance of smart wearable devices: An expectation-confirmation model approach. *Telematics and Informatics, 47,* 101318. https://doi.org/10.1016/j.tele.2019.101318

Peterson, J. (2019). Presenting a aualitative study: A reviewer's perspective. *Gifted Child Quarterly, 63*(3), 147–158. https://doi.org/10.1177/0016986219844789

Petroia, A., & Banu, I. (2019). The risks of cybersecurity of financial institutions and possible methods for their elimination. *Economica, 4*(110), 156–163. https://doaj.org/article/63bd8505f39478cb8a3cb6c1d8db390

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

Pham, H., Brennan, L., & Furnell, S. (2019). Information security burnout: identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications, 46*, 96–107. https://doi.org/10.1016/j.jisa.2019.03.012

Ponemon Institute. (2018). *2018 Cost of data breach study: Global Overview.* 2018 Cost of data breach study. https://tinyurl..com/y2ndae9b

Prentice-Dunn, S., & Rogers, R. (1986). Protection motivation theory and preventative health: Beyond the health belief model. *Health Education Research, 1*(3), 153–161. https://doi.org/10.1093/her/1.3.153

Queirós, A. F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Jounal of education Studies*, *3*(9). https://dx.doi.org/10.46827/ejes.v0i0.1017

Ram, M. K., & Selvabaskar, S. (2022). Digital technology adoption and its usage among unorganized retailers. *2022 Interdisciplinary Research in Technology and Management* (IRTM). https://doi.org/10.1109/IRTM54583.2022.9791591

Ramesh, G., Logeshwaran, J., & Aravindarajan, V. (2023). A secured database monitoring method to improve data backup and recovery operations in cloud computing. *BOHR International Journal of Computer Science, 2*(1), 1–7. https://doi.org/10.54646/bijcs.019

Renz, S., Carrington, J., & Badger, T. (2018). Two strategies for qualitative content analysis: An intramethod approach to triangulation. *Qualitative Health Research, 28*(5), 824–831. https://doi.org/10.1177/1049732317753586

Reyes, V. (2018). Three models of transparency in ethnographic research: naming place, naming people, and sharing data. *Ethnography, 19*(2), 204–226. https://doi.org/10.1177/1466138117733754

Ridder, H. (2017). The theory contribution of case study research designs. *Business Research*, *10*, 281–305. https://doi.org/10.1007/s40685-017-0045-z

Robertson, R. A. (2012). Security auditing: the need for policies and practices. *Journal of Information Privacy & Security, 8*(1), 30–37. https://doi.org/10.1080/15536548.2012.11082760

Sain, M. N., Normurodov, O., Hong, C., Hui, K. L. (2021). A survey on the security in cyber physical system with multi-factor authentication. *23rd International Conference on Advanced Communication Technology (ICACT).* https://doi.org/10.23919/ICACT51234.2021.9370515

Saini, K., Kalra, S., & Sood, S. K. (2022). An integrated framework for smart earthquake prediction: IoT, fog, and cloud computing. *Journal of Grid Computing, 20*(2), 17. https://doi.org/10.1007/s10723-022-09600-7

Santos, K. da S., Ribeiro, M. C., Queiroga, D. E. U. de, Silva, I. A. P. da, & Ferreira, S. M. S. (2020). The use of multiple triangulations as a validation strategy in a qualitative study. *Ciencia & Saude Coletiva*, *25*(2), 655–664. https://doi.org/10.1590/1413-81232020252.12302018

Sawatsky, A. P., Ratelle, J. T., & Beckman, T. J. (2019). Qualitative research methods in medical education. *Anesthesiology*, *131*(1), 14-22. https://doi.org/10.1097/ALN.0000000000002728

Scharp, K. M., & Sanders, M. L. (2018). What is a theme? teaching thematic analysis in qualitative communication research methods. *Communication Teacher*, *33*(2), 117–121. https://doi.org/10.1080/17404622.2018.1536794

Schneckenberg, D., Benitez, J., Klos, C., Velamuri, V., & Spieth, P. (2021). Value creation and appropriation of software vendors: A digital innovation model for cloud computing. *Information & Management, 58*(4). https://doi.org/10.1016/j.im.2021.103463

Silic, M., & Lowry, P. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems, 37*(1), 129–161. https://doi.org/10.1080/07421222.2019.1705512

Sinha, I., & Mukherjee, S. (2016). Acceptance of technology, related factors in use of off branch e-banking: An Indian case study. *Journal of High Technology Management Research*, *27*(1), 88–100. https://doi.org/10.1016/j.hitech.2016.04.008

Siwale, M. (2022). Applying technology acceptance model to measure online student residential management software acceptance. *Journal of International Technology & Information Management, 31*(2), 22–47. https://doi.org/10.58729/1941-6679.1547

Spiers, J., Morse, J., Olson, K., Mayan, M., & Barrett, M. (2018). Reflection/commentary on a past article:"verification strategies for establishing reliability and validity in qualitative research". *International Journal of Qualitative Methods*, *17*, 1–2.

https://doi.org/10.1177/1609406918788237

Srivastava, N. (2021). Cybersecurity: disaster recovery plan to protect business and ransomware. *ISSA Journal, 19*(2), 22–25.

Starks, H., & Trinidad, S. B. (2007). Choose your method: A comparison of phenomenology, discourse analysis, and grounded theory. *Qualitative Health Research, 17*(10), 1372–1380. https://doi.org/10.1177/1049732307307031

Stenfors, T., Kajamaa, A., & Bennett, D. (2020). How to... assess the quality of qualitative research. *The Clinical Teacher, 17*(6), 596–599. https://doi.org/10.1111/tct.13242

Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2022). Key factors driving the adoption of behavioral biometrics and continuous authentication technology: An empirical research. *Information & Computer Security, 30*(4), 562–582. https://doi.org/10.1108/ICS-08-2021-0124

Sungur-Gul, K., & Ates, H. (2021). Understanding pre-service teachers' mobile learning readiness using theory of planned behavior. *Educational Technology & Society, 24*(2), 44–57 .

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Tam, C., de Matos Conceicao, C., & Oliveira, T. (2022). What influences employees to follow security policies? *Safety Science, 147*, 105595. https://doi.org/10.1016/j.ssci.2021.105595

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems, 98*, 660–671. https://doi.org/10.1016/j.future.2019.03.042

Theofanidis, D., & Fountouki, A. (2018). Limitations and delimitations in the research process. *Peripherative nursing, 7*(3), 155–163. https://doi.org/10.5281/zenodo.2552022

Thomas, G., Burnmeister, O., & Low, G. (2019). The importance of ethical conduct by penetration testers in the age of breach disclosure laws. *Australasian Journal of Information Systems, 23(0)*. https://doi.org/10.3127/ajis.v23i0.1867

Thu Yein Win, T. H. (2014). Virtualization security combining mandatory access Control and virtual machine introspection. *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, Utility and Cloud Computing (UCC)*. https://doi.org/10.1109/UCC.2014.165

Tiwari, H., & Raman, R. (2022). Success attributes of business leaders from information technology industry: Evidence from India. *International Journal of Information Management Data insights, 2*(1), 100083. https://doi.org/10.1016/j.jjimei.2022.100083

Tomono, A. U., Uehara, M., Shimada, Y. (2010). A proposal for collecting many kinds of logs for internal control. *13th International Conference on Network-Based Information Systems, Network-Based Information Systems (NBiS)*. https://10.1109/NBiS.2010.39

U.S Department of Health and Human Services. (1979). *The Belmont Report.* Retrieved from https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf

Urban, J. B.-M. (2008). Choosing whether to use a qualitative, quantitative, or mixed-method approach. In J. B.-M. Urban, *In Designing and proposing your research project* (pp. 25–34). American Psychological Association. https://doi.org/10.1037/0000049-004

Van de Wiel, M. W. (2017). Examining expertise using interviews and verbal protocols. *Frontline Learning Research, 5*(3), 112–140. https://doi.org/10.14786/flr.v5i3.257

Van den Hoonaard, W. C. (2008). e-imagining the "subject:" conceptual and ethical considerations on the participant in qualitative research. *CIENCIA & SAUDE COLETIVA, 13*(2), 371–379. https://doi.org/10.1590/S1413-81232008000200012

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computer & Security*, *105*, 102239. https://doi.org/10.1016/j.cose.2021.102239

Velagapudi, S. L., Gupta, H. (2019). Privacy, security of cookies in http transmission. *2019 4th International Conference on Information Systems and Computer Networks (ISCON).* https://doi.org/10.1109/ISCON47742.2019.9036289

Vijayakumar, P., Moorthy, C. S., Upadhyaya, M., Dadheech, P., Yuvaraj, T., & Kshirsagar, P. (2022). Network security using multi-layer neural network. *AIP Conference Proceedings. 2393*, p. 020089. AIP Publishing LLC. https://doi.org./10.1063/5.0074089

Wang, L. (2017). Big data in intrusion detection systems and intrusion prevention systems. *Journal of Computer Networks, 4*(1), 48–55. https://doi.org/10.12691/jcn-4-1-5

Wibowo, F., Nuha, H. H., Wibowo, S. (2020). Network security analysis using https with ssl on general election quick count website. *IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*. https://doi.org/Comnetsat50391.2020.9328940

Wijitrisnanto, F., Suhardi, Yustianto, P. (2020). HTTPS contribution in web application security: A systematic literature review. *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*. https://doi.org/10.1109/ICITSI50517.2020.9264971

Wilson, A. (2015). A guide to phenomenological research. *Nursing Standard, 29*(34), 38–43. https://doi.org/10.7748/ns.29.34.38.e8821

Xing, Y. (2022). Design of a network security audit system based on log data mining. *Wireless Communications and Mobile Computing*, *2022*, 1–7. https://doi.org/10.1155/2022/6737194

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving cyber supply chain security. *IEEE Access*, *9*, 94318–94337. https://doi.org/10.1109/ACCESS.2021.3087109

Yeong, M., Ismail, R., Ismail, N., & Hamzah, M. (2018). Interview protocol refinement: Fine-tuning qualitative research interview questions for multi-racial populations

in Malaysia. *The Qualitative Report, 23*(11), 2700–2713. https://doi.org/10.46743/2160-3715/2018.3412

Yildiz, A. (2020). A discussion on accurate and effective data collection for qualitative research. *Journal of Current Research on Educational Studies, 10*(2), 17–24.

Yin, R. (2014). *Case Study Research: Design and Methods.* Sage.

Yin, R. K. (1981). The case study crisis: Some answers. *Administrative Science Quarterly, 26*(1), 58–65. https://doi.org/10.2307/2392599

Yoo, J., & Jung, Y. (2019). Interactive effects of organizational goal orientations on bank-employee's behavior. *International Journal of Bank Marketing, 37*(2), 402–425. https://doi.org/10.1108/IJBM-08-2017-0177

Zhou, X. (2020). Improvement of information system audit to deal with network information security. *2020 International Conference on Communications, Information System and Computer Engineering (CISCE)*. https://doi.org/10.1109/CISCE50729.2020.00025

Appendix A: Interview Protocol

Interview: Strategies to implement proper security for small financial institutions

Participate ID:_____ Date:_____ Start Time:_____Closing Time:_____

1. Introduction of myself and describe my role as the researcher
2. Verify Informed consent form has been signed
3. Remind participant of confidentiality and their right to withdraw
4. Remind participant the interview will be recorded for transcribing later
5. Discuss my research topic to ensure the participant knows what our conversation is supposed to surround
6. Go through each interview question
7. Thank the participant and schedule a follow-up date for communication regarding my interpretation of the transcribe interview.

Follow-up Communication Protocol:

1. Thank the participant again for meeting.
2. Go over each interview question and provide my interpretation ensure all interpretations are accurate, if any changes are needed document them.

Thank the participant for partaking in the study and provide contact information for any further questions they might have.

Appendix B: Interview Questions

Interview Questions

1. What techniques do you use assess vulnerabilities?
2. What strategies are you applying to mitigate vulnerabilities?
3. What strategies are you using to prevent outside threats?
4. What strategies are you using to prevent internal threats?
5. How do you handle vendor remote management?
6. What strategies do apply to remote work?
7. What strategies do you implement for secure communication?
8. What strategies do you implement for Disaster recovery?
9. What level do you feel your current strategies protect you from threats?
10. What level do you engage end user feedback on existing security measures such as guidelines they must adhere to?
11. What strategies have you implemented that failed?
12. What challenges do you face with your current strategies?
13. What are some setbacks you have experienced after applying new security strategies?
14. What is some skill sets you think an IT security professional should posse?