6-12-2024

Strategies and Methods Used by Information Technology Security Professionals to Secure Cloud Access Infrastructure

Oliver Fontem
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Oliver Fontem

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. Ayegbeni Igonor, Committee Chairperson, Information Technology Faculty
Dr. Patrick Mensah, Committee Member, Information Technology Faculty

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

Walden University
2024

Abstract

Strategies and Methods Used by Information Technology Security Professionals to Secure Cloud Access Infrastructure

by

Oliver Fontem

MS, Catholic University of America, 2006

BS, University of Calabar, 1993

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

June 2024

Abstract

Cloud computing provides data storage and access services to end users and enterprises but requires effective access controls to protect privileged information from unauthorized and malicious users. Enterprises adopt and integrate cloud computing into their business operations due to its cost-effective and on-demand delivery of computing resources over remote networks but face the challenge of adequate strategies and policies to implement identity and access management securely. Grounded in the Unified Theory of Acceptance and Use of Technology, the purpose of this qualitative multiple case study was to explore strategies used by information technology cybersecurity professionals to improve identity and access management in the cloud. The participants were 10 IT cybersecurity professionals, each with at least 3 years of experience in managing and implementing cloud security strategies and employed within the contiguous United States. Data were collected using semi-structured interviews and a review of publicly available information and analyzed using methodological triangulation. The results identified seven primary themes: (a) data protection, (b) authentication and authorization, (c) input and output handling, (d) error handling and logging, (e) configuration and operations, (f) session management, and (g) access control methods. A key recommendation is for enterprises to manage the human factor which can be unintentional human error or a disgruntled employee. The implications for positive social change include the potential to provide cloud service providers with strategies to secure their infrastructures and protect the private information of users and society from cyber criminals.

Strategies and Methods Used by Information Technology Security Professionals to Secure Cloud Access Infrastructure

by

Oliver Fontem

MS, Catholic University of America, 2006

BS, University of Calabar, 1993

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

June 2024

Dedication

To him who is able to keep me from falling, and to present me faultless before the presence of his glory with exceeding joy, to the only wise God our Savior, be glory and majesty, dominion and power, both now and ever. Amen.

Acknowledgments

I express my sincere thanks to the entire team at Walden University, particularly my committee members, Drs. Igonor and Mensah, whose guidance and insights enabled me to complete this program.

The members of Next Generation Cyber Engineers group who, despite their busy schedules, took the time to respond to surveys and follow-up interviews, without whom I would have had no content for my dissertation.

My colleagues at work, especially my supervisor, Tawanda Johnson, who supported and put up with my stresses during this study.

And my biggest thanks to my family for all the support. For my kids, sorry for being even grumpier than usual during this lengthy program. And for my wife, Miranda, thanks for all your support. To my dear sister, Ankwetta Fotabong Defang (Fontem Beatrice), thank you immensely for your moral support and for writing the checks for this program. You have been amazing. To my loving mother, who tilled the soil and remained stoic throughout the years to keep me in school and alive. To my brother, Denis Nkengafac, thank you for being so inspiring during your short span on earth with your eternal love.

Table of Contents

Section 1: Foundation of the Study

Cloud computing, a ubiquitous web-based technology service that provides data storage and access services to end users and enterprises, requires access controls to protect privileged information from unauthorized and malicious users (Jalili et al., 2019). Any enterprise that adopts and integrates cloud computing into business operations must adjust its information technology policies and practices to ensure the confidentiality, integrity, and authenticity of stored and accessed information. Though enterprises are unique in institutional culture, they face the same cybersecurity risks and challenges when adopting the cloud and need customized strategies and policies to protect privileged information. Kang and Hovav (2020) stated that it is essential for organizations to benchmark their information security policies because every organization has a unique policy that if pooled together can become an operational library of the standards, baselines, and best practices of information to a particular industry or market. Such a cumulative knowledge repository of benchmarks can pave a way for the design and implementation of more efficient information security policy guidelines, procedures, and standards. Because of increasing cyber threats and breaches, service providers need to guide and protect their networks preventively and proactively. Jeyaraj et al. (2021) stated that an organization's response to a cybersecurity event or incident refers to those actions taken to prevent, monitor, detect, mitigate, and manage cybersecurity threats and to recover from a breach.

Cybersecurity research has increased exponentially within the last decade due to increasing threats from threat actors. However, few studies have focused on the strategies

and policies needed to manage access controls. The COVID-19 pandemic forced companies to resort to remote work, and with this trend continuing unabated, the need for secure and reliable access controls has become a sine qua non. Tasheva (2021) stated that in 2020, there was an exponential increase in the scale and magnitude of cyberattack here threat actors exploited public health crisis fears and sent fake and alarming COVID-19 informational messages using social engineering tactics such as phishing to steal personal and corporate information or install malware on the device in use.

Background of the Problem

Cloud computing is a revolutionary opportunity for economic growth and social change for institutions of all sizes, private or public entities, and the general community. A significant benefit of cloud technology is that institutions use the cloud instead of investing in costly in-house data center solutions because the cloud's flexible infrastructure provides a combination of modernized computing, networking, and storage services (Harmon, 2018) Salat et al. (2023) stated that businesses have integrated cloud services into their operations due to the cloud's cost-effectiveness, flexibility, and scalability, which has witnessed continuous growth in the last decade. Matar et al. (2020) stated that organizations use information technology to provide better communication and automation for business procedures and processes. Though the cost of implementing information technology solutions is enormous, organizations that invest in cloud solutions experience increased value (Golightly et al., 2022). Jin and Bai (2022) used the difference-in-differences estimator to prove that cloud adoption results in about 6.9% improved sales, which is large-scale firm-level evidence on firm performance because of

cloud technologies with statistically significant positive short- and long-term effects. Wallis and Dorey (2023) stated that those who provide and manage critical infrastructure are responsible for mitigating the impact of cybersecurity events in their environments, including essential services they provide. Bhatti et al. (2021) stated that though outsourcing is the core of cloud computing and is vastly popular, it has a high failure rate, requiring research to understand the reasons behind such failures.

As service providers struggle to manage eminent risks from cloud computing services, it is essential to implement a reliable service delivery system that can be trusted by entities that are the service buyers and end users. Alshabib and Martins (2022) stated that in recent years, rates of cybercrime and cyber threats have increased exponentially, threatening the security and economic performance of governments, corporations, and the general global society. Loishyn et al. (2021) stated that to implement and manage a cybersecurity platform successfully, there is a need for research to capture cyber events, study them, and analyze the development and root causes for their occurrence to design effective countermeasures. Solms et al. (2011) stated that information security governance has emerged as a big problem in strategic management because it is critical in protecting a business's information assets. A correctly implemented information security governance framework should facilitate implementing and complying with strategic-level management directives.

Though cybersecurity is still in its infancy, research on information technology technological advancement, information technology infrastructures, governance, and implementation strategies abound. However, research on cloud security is limited and has

varied on cloud security implementation. Li et al. (2021) stated that some of the consequences of security incidents to organizations and their stakeholders are that security incidents incur costs in the form of damage control and information technology security-related investments because such investment decisions demand an evaluation of the system, risk factors, and the effectiveness of hardware and software. A global shortage of almost 3 million cybersecurity professionals was estimated in 2022 as organizations faced difficulties with the global health crisis. information technology curriculum should be in sync with business and industry needs to prepare information technology graduates with competencies and capacity-building skills to meet the demands of cybersecurity careers (Towhidi & Pridmore, 2023). The current study examined cloud security practices and policies used to secure cloud computing and the problems cloud security professionals face when protecting cloud stored information.

Problem Statement

The general information technology problem that prompted a literature search on this topic was that businesses that migrate to the cloud with critical business missions face the challenge of adequate strategies and policies to secure identity and access management in the cloud. Information technology security professionals need effective strategies to implement system access controls to improve cloud security. The literature indicated that the cloud infrastructure and its accompanying services provide access services and resources for many organizations and improve society's living standards. However, threat actors have breached and continue to pose security concerns for users. Cloud infrastructures come with access vulnerabilities that require access controls to

safeguard data. Arroyabe et al. (2023), in a 2018-2019 survey of 4,163 UK organizations, examined how cyber threats and attacks force corporate bodies to invest to protect their information systems and concluded that strategic cybersecurity investment is proven by both its role in organizational performance and the decision-making influences or factors. The current study examined cloud security practices and policies used to secure cloud computing and the problems cloud security professionals face when protecting cloud stored information.

Purpose Statement

This qualitative case study explored information technology cybersecurity professionals' strategies to secure access controls in the form of identity and access management in the cloud. The population under study was information technology professionals who manage and implement strategies and policies to secure access and protect data on the cloud infrastructure. The study population was composed of security information technology professionals employed by IT services with a minimum of 5 years of experience and expertise in managing identity and access policies and controls in the cloud and were employed by state or private sectors in contiguous United States. The findings from this study may contribute to social change by providing online shoppers, social media users, and the everyday internet user with strategies to secure their private information from cybercriminals. Using recommendations on identity and access management policies and best practices from this study may enable cybersecurity professionals to provide secure and protected cloud services for a better society.

Nature of the Study

A qualitative method was appropriate to obtain detailed information from information technology professionals using one-on-one open-ended interview questions about their experiences and practices in managing cloud security. The qualitative method was a good fit for this study because although the quantitative method is probability and statistics based, the qualitative method is used to gain an understanding of the thoughts and beliefs of participants and recognize the meaning that people attribute to their experiences (Batyashe & Iyamu, 2021). The quantitative approach typically requires an original hypothesis along with a plan for using numerical data. Because the current study was not designed to confirm or refute a hypothesis, the quantitative method was deemed inappropriate for this study. The qualitative method allows researchers to interact with participants through face-to-face interviews or focus groups in person, virtually, or via telephone (Segun, 2022). Case study research is a detailed investigation that requires a substantial period to conduct the study and often with empirical material collected from a well-defined case to analyze the context and processes involved in the phenomenon (Chowdhury & Shil, 2021). The case study method is a good fit for information technology research, considering that studying information systems as a discipline has shifted to organizational rather than technical issues (Rashid et al., 2019).

The qualitative method was appropriate for this study because I sought to collect data from current information technology professionals on the strategies they use to secure cloud platforms. An organization's information technology strategies on cloud computing and connected cloud network should have value, visibility, accessibility,

dimensions, and suitability (Li et al., 2021). The quantitative method was not feasible because its focus is on the probability and statistical components of the data gathered (see Goertz & Mahoney, 2013). I used multiple case studies to perform research on multiple cloud security professionals employed at two medium-size businesses using one-on-one interview questions.

Research Question

What strategies do cloud information technology professionals use to implement secure access methods to protect data in their cloud infrastructure?

Interview Questions

1. Tell me something about yourself, your company, and your background in cybersecurity.
2. How much experience do you have managing cloud security in general and cloud identity and access management in particular?
3. What challenges have you experienced since you migrated to the cloud?
   a. Can you describe some specific incidents you have encountered since migration?
4. How do you protect your system against unauthorized access?
   a. What factors do you consider when developing strategies and policies to protect your system against unauthorized access?
5. What techniques have you found most effective in designing and implementing adequate access controls?

a. Briefly, what is the most critical issue you want to address concerning access control, and what techniques do you intend to apply?
b. Why is the technique you have chosen more likely to succeed than other approaches?
c. Have you already done a feasibility test of this technique?
d. Why does this technique give you a competitive edge in the industry? How do you see this change impacting the field?

6. What are the challenges relative to the strategies used in designing and implementing access control policies?

a. How do you handle user access complaints?
b. What are the most common access complaints you receive from users?

7. What types of training do you offer to staff and system users on access control best practices, especially password complexity?

a. For training and compliance to succeed, you have to be keen to develop collaborations between departments. What opportunities for interdepartmental cooperation exist?
b. How do you fit in with the existing organizational structure? Who are your collaborators or people you expect to collaborate with within your environment? Why do you want to collaborate with them?

8. How does the general shortage of cloud security professionals or experts affect your business model?

a. What is the management position on training and grooming in-house staff to fill these vacancies?
b. With staff shortage, how do you balance your time? How would you prioritize if several challenges came up simultaneously (upgrade/patch management deadlines, zero-day incidents, corporate meetings, teaching commitments)?

9. Is funding a barrier to hiring and retaining talented and experienced cyber engineers? If so, how do you intend to solve this problem?

a. How do you convince management to accept to fund your project instead of other departmental priorities?

10. What additional information about your experiences protecting your system against unauthorized access would you like to share?

a. What would you do differently if you were starting your job again today?
b. What do you see yourself doing in 10 years? What are your professional goals in the next 5 to 10 years?

Conceptual Framework

Venkatesh et al. (2003) introduced the unified theory of acceptance and use of technology (UTAUT) under the User Acceptance of Information Technology: Toward a Unified View developed from eight renowned technology acceptance modes. Dwivedi et al. (2017) stated that the UTAUT was modified in 2012 and renamed the extending unified theory of acceptance and use of technology (UTAUT2) with the constructs of performance expectancy, effort expectancy, and social influence, which are factors that measure the behaviors and intentions of users and facilitate conditions that directly

influence user behavior with gender, age, experience, and voluntariness as moderating variables. Valerie et al. (2021) used the extended UTAUT2 framework to study the acceptance of the Bukalapak e-commerce system, while Dwivedi et al. tested the revised model using data from 1,600 observations involving 21 relationships from 162 research studies on IS/IT acceptance and use and concluded that the model was meaningful for understanding IS/IT acceptance and use. The UTAUT was a valid instrument to determine how access controls and policy strategies are accepted and used.

Definitions of Terms

Authentication: To verify and confirm that a user is who they say they are based on information provided by the user. Authentication is an indispensable process that asks the customer to go through a manual process of generating shared keys that ensure the functioning and secure communication between the user and server to ensure that something or someone is who they claim to be (Li et al., 2021).

Authorization: A process and level of privilege to ensure that correctly authenticated users can access only the resources the owner has approved (Bruzgiene & Jurgilas, 2021).

Cloud computing: Functionality in which the internet is used to deliver virtual services and storage facilities, databases, networking, software, and analytics in the cloud to users. According to Park et al. (2022), the National Institute of Standards and Technology (NIST) defined cloud computing as a rapid resource delivery service that is also convenient and comprises the computer systems, such as networks, servers, storage devices, computer applications, and related service that are automated.

Information security: Measures and strategies to protect information services and information systems from user abuse practices such as unauthorized access and disclosure and service disruption aimed to maintain integrity, confidentiality, and availability (Bhatti et al., 2021; NIST, 2020; U.S. Government, 2017).

Information security policy: Procedures, policies, and strategies designed to provide direction and guidance to manage information security risk (Kang, 2022).

Implementation strategy: Methods, actions, and processes implemented to overcome information security barriers, increase performance and implementation effectiveness, and sustain interventions over time to secure a cloud infrastructure (Szczepaniuk & Szczepaniuk, 2021).

Perceived ease of use: The ease with which a user believes that a piece of technology is easy or difficult to use and how that technology is expected to reduce effort. Perceived ease of use of a given technology increases with the intention to use the technology (Chatti & Hadoussa, 2021).

Perceived usefulness: How much a particular technology is expected to increase and improve job performance (Chatti & Hadoussa, 2021).

Security awareness: How a user is aware or familiar with an institution's mission, users, and employees (Bauer et al., 2017).

Unified theory of acceptance and use of technology (UTAUT): This theory is used to determine a person's intention to use technology and to show the associated relationships between effort expectancy, performance expectancy, behavioral intention, facilitating conditions, and social influence (Popova & Zagitova, 2022)

Assumptions, Limitations, and Delimitations

Assumptions

Research has three main assumptions: epistemological assumptions define what can be known, axiological assumptions define what is essential and valuable in research, and methodological assumptions define what methods and procedures are acceptable within the paradigm (Cherry, 2023). I assumed that the information pertaining to breaches and attempted breaches gathered by organizations participating in this study had been accurately detected, documented, and stored. Additionally, I expected that interview participants would respond truthfully to questions without any fear or bias influencing their answers.

Limitations

Limitations are factors that may hinder or weaken a study (Cunha & Miller, 2014). Because I relied on participant self-report methods for data collection, the study was faced with the challenge of a respondent responding to questions honestly. I expected that some interviewees may provide answers to please me instead of answers that were based on experiential learning. I also knew that interviewees may provide inaccurate or false answers to protect institutional reputation. The sample size was based on businesses in the contiguous United States that use cloud technology, which limits the study's ability to be duplicated in global geographic locations.

Significance of the Study

Contribution to Information Technology Practice

With technological advancement, the convenience of cloud-based computing with always-on connectivity has changed the manner in which traditional information technology security has been implemented and practiced. However, this functionality creates new loopholes and vulnerabilities that can be exploited by threat actors, which requires new measures to secure the cloud platform. Technological advancement has also enabled the creation and growth of digital tools whereby new releases of software and hardware, and the emergence of internet of things that has digitized home and social services and has effectively forced social change in the manner in which the society manages sedentary lifestyles, has led to increased need for cybersecurity in which the detection of known or existing vulnerabilities and zero-day attacks becomes a challenge for cybersecurity professionals (Peppes et al., 2023). Many global businesses are small and medium-size institutions that need research-based knowledge and solutions to understand the costs and reputational impact possible cyberattacks on their businesses and assets (Alharbi et al., 2021). Cyberattacks and security events have enormous consequences for businesses and related stakeholders, which cause increases in investments in information security. Information technology security investments' decision making is usually based on a careful evaluation of risk factors, the effectiveness of existing solutions, and evidence-based practices (Li et al., 2021). The literature indicated the need for a balance between security and ease of use using best practices to

design and provide solutions that feature both security or usability, but existing solutions tend to focus on either security or usability and not both (Faily & Flechais, 2011).

Some technology advancements have changed and benefited society including the health care sector, such as the emergence and use of the electronic health record (EHR) to reduce health care costs, improve the quality of care and the real-time delivery of health care services (Bhuyan et al., 2020). The EHR enables the use of sensor data and push notifications to detect fall incidents and provide real-time virtual care (M. Chen 2022). The introduction of the EHR has led to increased interconnectivity and interoperability of medical device information using the cloud platform but has also introduced security risks that pose a threat to the health care industry (Jones et al., 2022):

- Data storage: Traditional information technology models are designed based on costly and inflexible onsite data storage in contrast to cloud-based solutions that are more cost-effective in system development, reduced user control, and maintenance.
- Scaling speed: Cloud-based solutions are modular and can easily be commissioned and adapted to the unique organizational mission but pose security problems.
- End-user interfacing: Cloud platforms are interconnected with networks and services that must be secured. Risks range from unsecured end-user devices to software and network-level vulnerabilities to setup misconfigurations and user behaviors.

- Proximity to other networked data and systems: Cloud platforms are connectivity based between cloud providers and users; therefore, any defective device or wrong setup can be exploited, and privilege can be escalated to the entire system.

Implications for Social Change

Cybersecurity risks lead to consumer trust. A 2022 Consumer Reports survey of 2,103 U.S. adults reported that the last 3 years have seen significant changes to user cybersecurity practices due to a 44% increase in consumer online spending within 1 year. A breach will severely expose users' information, punish brands, and cause social mistrust. When people cannot afford fuel to automate their vehicles or learn that their bank accounts have been breached and their personal data found on the dark web, they experience firsthand the impact cyberattacks can have on their personal lives (Vijayan, 2023).

Data breaches come with psychological effects such as the WannaCry ransomware attack that led to disruption of critical infrastructure and critically impacted the U.K.'s National Health Service, particularly scheduled procedures. WannaCry's impact included disruption of critical systems, affected individuals, and created real-time awareness risks for many (Akbanov & Vassilakis, 2019). The WannaCry ransomware attack demonstrated how basic vulnerabilities in basic infrastructure could bring social change.

Cyber breaches cause service disruptions and depending on the nature of the breach, may be spread across a network, or limited to a local infrastructure, but are

frustrating to individuals directly affected. A 2019 ransomware attack on a software vendor affected 22 Texas towns. The cybercriminals demanded $2.5 million to restore administrative services, and effectively prevented residents from accessing records or paying utility bills (Bleiberg & Tucker, 2021). The current study was conducted to identify best practices that may mitigate the increasing number of breaches.

A Review of the Professional and Academic Literature

The objective of this literature review was to provide evidence on the topic under investigation through the identification and understanding of available cybersecurity research using online search strategies that uncovered systematic research that was relevant to my study. This rigorous literature review addressed a field of knowledge that has seen exponential growth. Clim et al. (2022) conducted a literature review of cybersecurity problems with a focus on smart cities and concluded that cities are using both existing and emerging technologies to implement cybersecurity solutions. This literature has been relevant in helping information technology managers and professionals develop strategies to identify, evaluate, and analyze some of the issues that have been raised in conceptual and empirical discussions.

The current literature review was conducted using a systematic approach to collect extensive published works from various authors and to assess topics that need considerable analysis to understand. Alomari et al. (2021), in a systematic review of online published literature, identified peer-reviewed works on artificial intelligence (AI) and IAM and concluded that there is need to identify a service that can manage identity governance and access control. Bhatti et al. (2021) analyzed 63 papers published between

1994 and 2020 on research that addressed outsourcing information security risk management and found that most studies used conceptual models or provided commentary as a popular research methodology while other researchers collected secondary data instead of primary data directly from industry, and most did not investigate a specific industry or an information technology outsourcing client or service provider.

The current review of the existing literature was conducted to identify gaps in the research, to build a theoretical foundation for the topic under investigation, and to justify a need for the research and its contribution towards cybersecurity as an emerging field of study. Thoreau and Sage databases were searched using keywords and Boolean logic. Most of the articles came from the Walden University repository and some from Google Scholar. All articles were published in English, spanned global locations and internationally peer-reviewed journals, and were published within 5 years of the current study's completion date (2024). A critical evaluation of the titles, keywords, and abstracts eliminated results not relevant to this study. The review includes journals and book chapters but not conferences papers. After careful sorting, only 121 scientific studies were chosen and reviewed.

UTAUT

UTAUT is a theoretical model to determine the use of technology as a behavioral intention. UTAUT has four constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions) that help to determine the perceived likelihood of

adopting the technology. These predictor variables moderate experience, voluntariness of use, age, and gender (Venkatesh et al., 2003).

Performance expectancy is the measure of an individual's belief in the extent to which a piece of technology can help attain gains in job performance (Venkatesh et al., 2003) derived from technology acceptance model constructs (TAM), TAM2, model of PC utilization (MPCU), social cognitive theory, motivational model, innovation diffusion theory (IDT), and theory of planned behavior (CTAMTPB). Performance expectancy is a proven indicator of intention to use and is reliable in voluntary and mandatory environments (Venkatesh et al., 2016; Zhou et al., 2010). Effort expectancy is the measure of ease of use of any piece of technology (Venkatesh et al., 2003) derived as a construct from perceived ease of use and complexity from TAM, MPCU, and IDT. Over time, this construct becomes less effective and less significant due to familiarity with extended technology use (Chauhan & Jaiswal, 2018; Gupta et al., 2008).

Social influence is the measure of the value an individual perceives that other people believe they should adopt a new technology (Venkatesh et al., 2003). This construct is associated with the subjective norms, social factors, and image constructs used in TRA, TAM2, TPB, CTAMTPB, MPCU, and IDT because it indicates that people change their behavioral intentions and act according to the perception of others about them and how they believe others want them to behave. Social influence is the use of technology to comply with organizational mandates and not due to personal preference (Venkatesh et al., 2003). The construct's inconsistent effect was also confirmed by other studies that validated the model (Chauhan & Jaiswal, 2016; Zhou et al., 2010).

Facilitating conditions measure the extent to which a person perceives that an organization and its technical resources have the organizational culture and support structure to encourage technology use (Venkatesh et al., 2003). This construct derives from compatibility, perceived behavioral control, and facilitating conditions constructs from TPB, CTAMTPB, MPCU, and IDT. This construct positively influences the intention to use, though over time familiarity makes the effect less significant. Age, gender, experience, and voluntariness of use are predictors of intention because they exert a moderating influence. Age moderates the effect of all four predictors. Gender moderates the social influence, and experience moderates the relationships between effort expectancy, social influence, and facilitating conditions. Voluntariness of use has a moderating effect on the social influence and behavioral intention relationship only (Venkatesh et al., 2003).

The UTAUT model has contributed to the literature and has been used by researchers to provide empirical evidence for technology acceptance and to compare and contrast technology acceptance theories, such as to prove that proposed factors account for 70% of the variance in use intention (Venkatesh et al., 2003). The UTAUT model has been found to have better prediction compared to other models that have been tested on technology acceptance (Davis, 1993; Sheppard et al., 1988). With recent technological advances in the medical service field, the evolution of several varieties of ICT-based health information services has enabled real-time and intelligent customized services and has led to innovation in the medical service field across the world; however, its acceptance of use in low-income countries is still limited. Bramo et al. (2022) also

validated and used the UTAUT to sample opinions and attitudes in the primary health care industry in Ethiopia and concluded that although health care providers accepted ICT-based health information services consistent with the UTAUT, they experienced burnout due to additional clerical duties of data input, which is time-consuming and complex, and organizational culture such as leadership commitment. Chatti and Hadoussa (2021) researched Saudi university students' intention to use digital technologies during the COVID-19 pandemic. The UTAUT was validated using a combined factorial analysis and linear regression analysis; results indicated that five key factors had significant and positive effects on students' intent to use digital technology. These four factors included perceived usefulness, perceived ease of use, teacher influence, university management commitment, and availability of student technical assistance.

Aziz et al. (2022) used a UTAUT model questionnaire to investigate a sample of 321 Malaysian research university faculty's ethical, intentional, and behavioral patterns in adopting online educational technologies and concluded that ease of use, social influence, and ethical considerations significantly influenced behavioral intention and facilitating conditions had positive relationships with use behavior. Wang et al. (2021) reviewed 1,694 peer-reviewed articles from 2003 to 2021 that used the UTAUT and also tracked the evolution and characteristics of the UTAUT and concluded that it was essential for researchers to provide users with a better experience through information technology to understand the topical research evolution related to the UTAUT model. Performance expectancy is the measure of an individual's belief that there will be gains

in job performance if the system is used, which researchers have indicated has a positive relationship with behavioral intention (Popova & Zagulova, 2022).

UTAUT2 and Its Extensions

The original UTAUT framework was designed with a focus on the acceptance of technology in an organizational environment (Venkatesh et al., 2003) but was later applied in nonorganizational environments (Venkatesh et al., 2012; Venkatesh et al., 2018). UTAUT has been used in the literature in a broad context, thereby enhancing its generalizability as a theory (Venkatesh et al., 2012). Also, the discipline of information communication technologies and technological advancement has seen researchers adapting the UTAUT to other contexts and improving its predictability (Venkatesh et al., 2012). Though these adaptations helped to expand the knowledge base and made the UTAUT more understandable, research was generally focused on organizational environments (Chang, 2012). There was a need for further research to provide evidence to support a user behavioral model for the use of technology in noncorporate environments, such as consumers or the general community. The emergence of the Internet of Things, e-commerce, and social media platforms has caused an exponential increase in the use of technology by the public. Research has suggested that there is a significant difference in the determinants of technology acceptance in organizational and nonorganizational contexts because there is a variance of context between predictive factors such as costs and benefits of behavior (Brown & Venkatesh, 2005).

As a result of these limitations, Venkatesh et al. (2012) proposed an extension of UTAUT. The new model, named UTAUT2, added three constructs, changed some

relationships, and removed voluntariness from the original model to make it adaptable to a consumer technology use environment, which helped to advance the technology acceptance literature (Venkatesh et al., 2012) and provided broader generalizability to private user environments. The three new constructs were hedonic motive, cost/perceived value, and habit moderated by age, gender, and experience. Hedonic motivation measures the enjoyment of use and acceptance of technology and has proven to be a reliable indicator (Venkatesh et al., 2012). Information science and marketing research has provided literary warrant to justify the perceived hedonic nature of the outcome, such as perceived enjoyment, to be a significant predictor of consumer technology use (Brown & Venkatesh, 2005). The construct of cost/value was justified based on the concept of consumer product use in organizational environments because it was shown that workers who use an organization's technology assets do not feel responsible for its cost or value because the employee does not feel burdened by any direct financial implications (Venkatesh et al., 2012). Price value measures the value of a user's perceived benefits of using technology and the related monetary value (Venkatesh et al., 2012). Habit measures the extent to which a user exhibits spontaneous behaviors (Venkatesh et al., 2012). This construct had evidence from prior research because it was used in a hypothesis to affect use directly and indirectly through behavioral intention (Venkatesh et al., 2012).

Dwivedi et al. (2020) studied the selection of an appropriate theoretical model to assess the acceptance and use of technology using the UTAUT and, based on the synthesis and review of 162 studies, developed a modified version (meta-UTAUT). Findings suggested that a growing number of studies have cited the relationships, and

researchers have reviewed it alongside other alternative models while analyzing acceptance and use of technology. Dwivedi et al. stated that they used qualitative methodology to determine cybersecurity use and acceptance, which further validated and provided literary warrant for the application of the UTAUT as a theory model.

Applications: UTAUT and UTAUT2 Used in the Literature

The generalizability of UTAUT and UTAUT2 has been tested within varied cultures and geographic environments to understand and provide evidence of the role of culture and geography in technology adoption (Gupta et al., 2008; Im et al., 2011; Venkatesh et al., 2012). Most studies found that the role of UTAUT constructs was significant across cultural settings. The model was used to compare the rate of technology acceptance between culturally and geographically diverse countries, the United States and China, and the results demonstrated an effective predictive measure of the model across cultures but accounted for a more significant variance in the behavioral intention when fewer moderators were tested (Venkatesh et al., 2012). A similar study using UTAUT comparing Korean and U.S. contexts found that the effectiveness of associated relationships slightly varied with an unvaried significance (Im et al., 2011). In another study using the UTAUT model to test cross-cultural influences in individualistic versus collectivistic societies, the model was proven viable across both cultures but with different relationship effectiveness, indicating a robust moderating role of culture (Udo et al., 2016).

UTAUT2 has also been tested and validated across geographic boundaries with known cultural differences and economic and technological advancement. Social

influence did not affect technology adoption in the banking industry in Jordan (Alalwan et al., 2017), but a comparative cross-national study of Korea, Japan, and the United States on the adoption of educational technology found variations across samples in the predictive power of the relationships and the significance of the effects (Jung & Lee, 2020). The intention to use e-learning correlated with the habit construct, while perceived efficacy was more predictive of Korean users. In contrast, Japanese users were affected by habit in behavioral intention, price value, and social influence, while U.S. users were affected by habit and price values. Effort expectancy was not significant across all three countries, though a reason may be that the tested technology was easy to use.

UTAUT and UTAUT2 models have been well researched and validated in various environments to examine technology acceptance, such as the health care sector (Chang et al., 2007), e-government (Chan et al., 2010; Gupta et al., 2008), mobile wireless networks (Venkatesh et al., 2012), enterprise systems (Chauhan & Jaiswal, 2018) and mobile banking and apps (Mütterlein et al., 2019; Zhou et al., 2010). Research has reported a UTAUT dependency of behavioral intention on the perception factors of perceived performance and perceived ease of use (Chang et al., 2007). The technology acceptance framework was applied to measure the acceptance of pharmacokinetics-based clinical decision support systems. Except for the facilitating conditions, whose influence was found only on the actual use of the technology, all other constructs had significant effects on the intention to use. A study to understand the adoption of e-government by public employees in a developing country found a significant influence of all UTAUT variables moderated by gender (Gupta et al., 2008). However, performance and effort expectancy

had more significant effects. Its application to measure the degree of acceptance of ERP software training indicated that three of the four predictors of use intention were significant, where effort expectancy, performance expectancy, and facilitating conditions significantly predicted employees' intention to adopt ERP tools, but social influence had no significant effect (Chauhan & Jaiswal, 2016). Chauhan and Jaiswal (2016) suggested that the findings may have been influenced by the instrumental nature of ERP software and the high contingency due to compliance factors that interfered with the user's intentional decision making. UTAUT2 has produced mixed results in behavioral determinants' significance and predictive value across cases.

UTAUT2, when applied to investigate mobile app adoption, found significant effects in performance expectancy, social influence, hedonic motivation, and habit (Mütterlein et al., 2019), though two studies that used UTAUT2 to investigate its adoption in the mobile banking sector could not confirm the role of social Influence (Ajzen, 2011; Baptista & Oliveira, 2015). The most significant effects were noted in the performance expectancy, hedonic motivation, and habit constructs (Baptista & Oliveira, 2015). UTAUT has tested validity for understanding the acceptance and successful usage of ICT-based services in low-income countries and is considered a validated and used model in technology acceptance research in the healthcare field (Bramo, 2022).

Limitations

The UTAUT is a proven holistic tool to measure the use and acceptance of technology (Venkatesh et al., 2003; Venkatesh et al., 2007). However, UTAUT suffers from some theoretical and methodological limitations that need further studies to research

and validate (Venkatesh et al., 2003; Venkatesh et al., 2007). Research evidenced concern regarding the broad application of UTAUT (Dwivedi et al.), who demonstrated that most information systems researchers cite the original UTAUT paper without using the model, resulting in overrated citations and doubts over its robustness (Dwivedi et al., 2019). As a result, an analysis of MASEM (Combined meta-analysis and structural equation modeling) proposed a revision of UTAUT to include attitude construct as a partial mediator of the effects of exogenous constructs on behavioral intentions (Dwivedi et al., 2019). UTAUT2 uses a self-reported scale to measure intention to use (Venkatesh et al., 2012), and a self-reported scale lacks accuracy and validity in addition to the threat of standard method variance (Straub & Burton-Jones, 2007; Sharma et al., 2009). Different methodological approaches have been recommended to reduce the potential of common method bias such as using experimental settings that can make manipulation checks possible.

Transition and Summary

Cloud Security

Cloud security is an emerging field in cybersecurity aimed at educating, training, and researching methods and strategies to secure cloud services that include data privacy, cloud infrastructure, cloud applications and platforms. Cybersecurity is the policies and procedures used by an organization to protect its interconnected systems exposed to cyber-threats. In practice, cybersecurity individuals and enterprises work in harmony to protect personal and corporate information, data centers, networked services, and critical infrastructure from unauthorized access by internal and external threat actors (Alazab et

al., 2022). Profit driven economic motivation in addition to industry and state regulatory mandates have caused companies to increasingly make cybersecurity a pivotal part of their strategic management and to take strategic measures to protect their information and infrastructural assets (Mirtsch et al., 2021). These systems and platforms are critical infrastructure assets of national interest, thus securing them requires the coordinated efforts of cloud providers and users, such as an individual, a business entity or government agency. Since the business mission of cloud providers is to provide host-based services to its clients, the success of a provider's business depends on customer trust. Trust means the cloud provider needs effective and reliable cloud security standards and strategies to protect and secure client data to ensure client trust by providing privacy and safety to stored data. However, the client and the user are also responsible for cloud security. Understanding cloud security from both ends is pivotal. Organizations must adopt standards, implement security controls, enforce compliance, and align technologies, processes, and people to conform to industry standards, local and national laws, and regulations to provide a cloud security solution that works. The effect of noncompliance on both individuals and organizations is hard to measure but in general the cost has risen sharply in recent years to an average of $14.82 million per organization in 2017 (Chen, 2022). 2020 witnessed an exponential surge in the number of cyber-attacks where malicious actors benefited from the public's COVID-19 health crisis fears to use phishing engineering techniques to send misleading COVID-19 information and urgent messages which enabled them to penetrate and access user information and, in some case, escalated privilege or installed malware on their devices (Tasheva, 2021).

Organizations need to and should implement continuous and persistent efforts to improve information security management by adopting researched and evidenced-based measures and approaches with proven effectiveness to secure and enhance information security and to sustain an organization's competitive advantage (Ghahramani et al., 2022). Upper Echelons Theory states that the characteristics of decision-makers partially determine an organization's performance, consequently, senior management team composition may play a decisive role in a firm's strategic policies and outcomes (Georg-Schaffner & Prinz, 2022).

Cloud security is categorized into:

- legal compliance
- identity and access management (IAM)
- business continuity and data retention
- information security
- governance

Cloud security integrates technology, protocols, and evidence-based practices to secure and protect cloud environments including applications, and stored data. To successfully manage a cloud environment, it is essential to understand what must be secured and the administrative practices, procedures, policies, standards, and strategies to manage and secure it. Processes that manage security vulnerabilities in the backend are the responsibility of cloud service providers, and clients are responsible for adopting and implementing safe use behaviors and proper configuration of end-user hardware and software. The scope of cloud security seeks to secure:

- physical networks: climate control, routers, cabling, and energy
- data storage: hardware and software
- servers: networks, hardware, and software
- virtualization machines and frameworks
- operating systems (OS), API management and runtime environments
- data: information at rest, in transit, modified, or accessed
- applications: software and related applications
- end-user hardware: computers, (IoT) devices, and mobile devices

Cloud computing is an emerging field where the definition of ownership over each component, the scope of the provider and client security responsibilities remain fuzzy. Since responsibility may depend on the degree of authority and control legally granted over each component, it is essential to understand how it is compartmentalized. Enterprise cybersecurity posture is the totality of all possible computing and networked security risks that result from staff risks behaviors and practices such as carelessness, mistakes, inexperience, insider threats, and vulnerabilities from social engineering (Alqahtani, 2022). Focusing only on interoperability and not paying sufficient attention to threat adversaries in a hostile environment is a mistake that cybersecurity professionals need to understand considering that so many networks are insecure. (Sobel & Vetter, 2022). A system is only as secure as it is configured with effective polices and controls because garbage-in spits out garbage. Data generated from a system mirrors data inputs, thus it is difficult to use collected systems data to figure out the inner workings of that system. Good and reliable data is very valuable, and the increasing value of data has

made big data a critical target for cyber-criminals (Rawat et al). Realizing a research topic is evidenced by the need to collect data from cyber-attacks, study and analyze the root causes for their occurrence and propose countermeasures (Loishyn et al., 2021). Since cloud security has witnessed continuous growth in software and infrastructure in the last decade, it has been embedded within businesses because it provides cost-effective, flexible, and scalable environments (Salat et al., 2023). Evidence shows that the negative economic impact experienced by breached firms spills over to a bystander firm in the same industry, a phenomenon known as industry contagion effect (Kelton & Pennington, 2020). A critical argument between developed and developing countries in their varying threat landscapes is that economic instability, high unemployment, and low wages are factors in developing countries that may induce individuals to engage in cyber-criminal activities. This makes it essential for cybersecurity decision makers to take in consideration the economic and political influences that may be a motivation to cyber threats and how this contributes to understanding specific issues that need to be factored into cybersecurity solutions (Hurel, 2022).

Cloud security is implemented in two ways. First, cloud service type modules create the cloud environment managed by third-party providers where each professional may have responsibility and exercise limited control over certain components of a service comprising the network infrastructure, storage facilities, servers, and virtualization. These services are provided to clients through the cloud and accessed remotely. Software-as-a-Service (SaaS) is provider-hosted applications in the cloud. SaaS services to clients are

data, runtime, middleware, and operating systems such as Google Drive, Cisco Webex, and Microsoft 365.

Platform-as-a-service (PaaS) are provider-hosted platforms for clients to develop their applications. PaaS runs on provider servers where the provider manages the runtime, middleware, and operating system from which the client can develop its applications within a client's environment. Client's responsibility is to manage applications, data, end-user access, networks and devices such as Windows Azure and Google App Engine.

Infrastructure-as-a-Service (IaaS) is a provider-hosted cloud-based hardware and operating system offered to clients who have remote access. The cloud provider manages core services in the cloud. The client is responsible for securing all stacks atop an operating system, such as the OS, middleware, applications, data, runtimes, and end-user devices, networks, and access. IaaS includes Microsoft Azure, Google Compute Engine (GCE), and Amazon Web Services (AWS).

Second, cloud environments are the different deployment options that host cloud services that end-users use to create a system and organizations, share management roles, and define the security responsibilities of clients and providers. Critical infrastructure is physical or virtual systems and assets that are vital and any failure through destruction or damage would severely impact the United States security, public health or safety, economic security, or a combination (USA Patriot Act, 2001). These cloud environments include:

1. Public cloud is multi-tenant cloud platforms that host multiple clients on a single provider's server. The provider runs these third-party services, and the client is provided access through the web.
2. Private third-party cloud is a single-tenant service where clients exclusively own and manage their cloud platform.
3. Private in-house cloud is a single-tenant service where servers are operated from a client's private data center and run by the client who has complete control over its configuration and setup.
4. Multi-cloud environments combine cloud services from different providers to form a hybrid of public/private services.
5. Hybrid environments combine third-party and onsite private cloud data centers.

The goals of all cloud security measures are to achieve the following:

- prevent data loss through data recovery solutions,
- protect data in storage and related networks against malicious acts,
- prevent insider threats, human negligence to safeguard data breaches,
- reduce the attack surface, mitigate impact of a breach, and rapidly respond to data or system disaster,

Data security as a field is concerned with how to technically secure data or prevent threats incidences from occurring. Technological advancements have provided clients and providers with tools and technologies to enact walls that separate internal and

external networks and applications to control access sensitive data and protect data in transit such as encryption and virtual private networks (VPNs) that are also encrypted.

Identity and access management (IAM) is a tool that authenticates and authorizes user accounts and grants access to authorized or legitimate users based on the principle of least privilege. Access controls are policies that are needed to control access to legitimate users and threat actors from accessing and compromising critical systems and privileged data. Some access control best practices are password management and multi-factor authentication.

Governance is a group of policies used in managing a system or network to detect, prevent and mitigate threats such as safe user behavior policies, access control policies, and user awareness training. Business continuity (BC) and data retention (DR) planning are entity-specific technical disaster recovery readiness plans intended to be implemented in case of data loss such as data redundancy through backups, systems redundancy to ensure availability, frameworks for testing and validating that controls and policies are doing what they were designed to do and employee recovery guidelines.

Legal compliance, such as HIPAA to ensure user privacy is a federal government law and industry specific standards such as SCALA standards designed which mandates that entities must explain why they need to collect a user's information, why it needs to be stored, and for how long and under what protective measures, such as data masking obscuring identity within data using encryption methods. Systems such as SCALA are based on the principle that a change from individual compliance to group mandates based on industry specific best practices is a preferable standard. Such standards see groups

working together in a coordinated manner where the individuals' combined beliefs and collective effort can produce desired information security performance goals and assessment effects (Yoo et al., 2020).

Cloud Security Risks

Knowing and understanding security issues in the cloud is essential because protecting what one does not know is nearly impossible. Privately owned critical infrastructures such as the financial networks, pipelines, and power grid managed through the cloud and open to cyber-attacks have in the last two decades been open to vulnerabilities, and the US has responded with several sector specific partnerships with private owner-operators of critical systems using varying degrees of regulations (Atkins & Lawson, 2021). The occurrence of data breaches today is no longer a question of if but a matter of when. Considering that the costs of an occurrence is huge and continues to increase, it is critical to plan and implement protective and preventative measures that can proactively respond to general and specific threats (Walton et al., 2021). Common cloud security threats include:

- Incompatible legacy systems and third-party service interruptions.
- Insider threats or system misconfiguration errors.
- External threats that include threat actors using malware, phishing, or DDoS attacks.
- Threat surface. Traditional measures aim to secure the perimeter, but with interconnected cloud environments and insecure APIs, account hijacks

become a significant security risk. Cybersecurity professionals must shift to a data-centric approach to effectively counter cloud security risks.

- Privilege escalation: Network interconnectivity means malicious actors can breach a network through compromised or weak credentials and use vertical or horizontal mobility to gain unauthorized access to critical information.

Third-party data storage implies that client access to the client owned data may be at risk if those services are interrupted which could result long-term repercussions. Cloud giant Amazon's cloud data facility servers recently incurred damage when it experienced a power outage and some of its clients suffered enormous data loss. This is why local backups of data and applications are redundant but necessary.

Telecommuting has increased exponentially due to COVID-19 health crisis government strictures. These increases in telecommuting have expanded the attack surface where remote access, videoconferencing software, personal devices and private Wi-Fi networks have opened new exploitable loopholes (Slapničar et al., 2022). Telecommuting, online shopping and social interaction have caused the digital economy to grow exponentially annually, thus making it imperative to conceptualize cybersecurity as a supply chain whose economic impact affects a more significant number of stakeholders within the supply chain (Farahbod et al., 2020). Attacks such as the Mirai Botnet or cardiac device vulnerabilities expose impact of having vulnerable or insecure cloud systems. There is therefore a critical need for risk assessment mechanism to evaluate the resilience of cloud infrastructure, cost of security risk to business and

individuals, prioritize and rank IT assets and measure them with standardized baselines (Shaikh & Siponen, 2023).

Why Cloud Security Is Important

The exponential increase in and the evolution of cybercrimes and the increasing cyber risks to the society has caused cybersecurity to become a hard to solve problem and a critical issue for both private and public decisions makers (Kianpour, 2022). Threat actors continue to target sizeable multi-organizational data centers, most are highly centralized and cause immense data breaches with financial and reputational consequences. As cloud computing services become increasingly popular in use, it increases the attack surface that will result technology leaks due the nature of cloud computing services as virtual resource for sharing and virtualization. Since cloud services are exposed to many emerging cyber-threats, current and would be adopters' companies become hesitant in embracing the cloud (Park et al. 2022). There is therefore a research need to investigate and develop effective solutions to mitigate such reliabilities. Threat actors have realized the value of cloud-based resources and are rapidly exploiting them. The emergence of advanced solutions that can help to identify and understand the impact of cyber-threats on organizations shall enable decision-makers to better prioritize and resolve threat incidents and events (Zadeh et al., 2020). The advancement of cloud technology makes it a sine qua non to reevaluate cyber security. Cloud stored data and applications flow from their stored locations to local users using remote capabilities which are always internet accessible. This makes protecting cloud stored data more problematic than when it was traditionally stored just on premise. There is need for a

structured assessment approach to facilitate the identification of causes and develop possible mitigation measures (Emer, 2021).

A comprehensive evaluation of a cloud infrastructure to measure resilience requires a particular security control and standards set to meet specified security requirements (NIST, 2023). Estimating the global state of a networked system is an essential problem in many application domains, but the current solution has been the periodic observation method, which has proven ineffective (Liu et al., 2021). It is for this reason that the Global Cybersecurity Index (GCI) was created to measure individual country's commitment to cybersecurity globally and to raise cybersecurity awareness (Bruggemann et al., 2022). The aim of information security risk management is to analyze and prioritize primary data to identify possible risk factors (Yang, 2022). The measure of the efficiency of a single security control can be seen its ability to mitigate the vulnerability of a system (Sawik & Sawik, 2022). Analyzing cybersecurity risks helps to identify potential vulnerabilities and threats that proactive measures can be implemented to secure the infrastructure and prevent potential attacks (Bouzidi et al., 2023). Real-time situational assessments of security events generated by network devices and applications and uploaded to a new generation of SIEMs built with automated response functionalities that select and deploy countermeasures are welcome, but they do not perform impact analysis and provide real-time responses to attacks (Gonzalez-Granadillo et al., 2021). Managing cloud security today mandates that cloud security professionals change some previous IT practices. The UK's Kaspersky anti-virus software, the US's Android operating system, the war in Ukraine, and China's bellicose attitude towards Taiwan have

exposed how essential the domesticity of digital products and the importance of establishing the origin of digital products for national cybersecurity have become (Ozdemir et al., 2022). Data transfer and interpersonal communication in business and social environments are interconnected online transactions that use publicly available infrastructure that is vulnerable and susceptible to and exposed to risks from external and internal threat actors or system failures that may result in workflow and critical infrastructures disruption (Turk et al., 2022). Internet usage witnessed a surge during the COVID-19 pandemic where stay at home government mandates saw even non-internet users relying on interconnected networks to communicate, shop and work and attacked by cybercriminals (Barik et al., 2022). Cloud computing is growing exponentially as the workplace and individual users increasingly rely on it for critical business functions and daily routines. Innovation leading to technological advancement is automating society at a geometric rate and much faster while the implementation of industry security standards and government regulations lack behind, leaving IT professionals with the responsibility to manage the risks of cloud accessibility where the development and stability of global information flow are threatened by ineffective cybersecurity strategies (Kianpour, 2022). This problem is further exacerbated by the global shortage of cybersecurity professionals, in which the gap between the demand for and supply of cybersecurity experts has increased by more than 50% from 2015 to 2021, where 62% of employers have reported a lack of cybersecurity talent (ISACA, 2020) (Towhidi & Pridmore, 2023). The evolving cybersecurity environment requires strategies to reduce risks and increase the resiliency of IT systems. The federal agency National Institute of Standards and Technology's

(NIST) Cybersecurity Framework seeks to address this need and offers guidance for improving risk management in critical infrastructures relevant to the government and the private sectors (Krutilla et al., 2021). IT professionals are bugged down by numerous challenges such as the uncertainty over the definition of such concepts as the cybersecurity concept itself and risk, ambiguity over the problem of specifying, building, and managing enterprise level security systems or managing security for devices of social significance such as Internet of Things (Villalón-Fonseca, 2022).

Cloud Security Awareness

Cloud security awareness should be integral to any organization's policy to protect its data and assets from cyber threats. Cloud security awareness training can help avoid costly data breaches by enhancing the knowledge base, skills, and professional behavior in the cloud environment. Online commerce is facing several inhibiting factors, such as the lack of security perception because the product is sold online (Cordente-Rodriguez et al.). Cloud security awareness education aims to increase an understanding of the risks, challenges, and best practices of cloud security comprising computing models, service providers, security standards, security controls, threats, and incident response. Cybersecurity outcomes are interconnected and predicated on the contributions and choices of disparate parties with user a never aware of how his or her immediate online actions, reactions and behaviors effects the planned controls and policies of IT professionals who defend the network or the disparate actions of other users (Dykstra, 2022). Even within IT professionals and particularly large departmental units at institutions such as colleges and universities, IT managers who lack interaction with other

departments do employ security strategies that are often ignored by other departments (Chapman &Reithel, 2021). Constraining factors at the personal and individual level such as cybersecurity knowledge, beliefs, cultural values, job attachment and satisfaction and organizational culture do impact an employee's compliance with an institution's information security policy (Nord et al., 2022). Information security policies are the ultimate strategies to protect an organization's assets, but organizational compliance is crucial for reducing information security incidents, and though information security managers have implemented information security awareness programs to ensure cybersecurity security information flow systematically and continuously to a target audience, more still needs to be done (Bauer et al., 2017).

There is need for professional development skills that should build competencies and capabilities to identify and avoid common cloud security pitfalls, such as misconfiguration, weak authentication, and unauthorized access, geared towards preventing, detecting, and responding to cloud security incidents. Cloud security professionals shall also gain confidence in using cloud services and tools securely and efficiently to develop a proactive attitude towards cloud security and data protection, foster a culture of collaboration among colleagues and stakeholders, and demonstrate a commitment and compliance to cloud security standards and regulations. Many studies recognize that the weakest link in a cybersecurity environment is the human factor (Szczepaniuk & Szczepaniuk, 2022). There is research evidence that learning from information security incidents and resolving root causes is a best practice, however, there is research evidence that many organizations do not learn from incidents but focus

attention instead on resolving the direct causes of incidents (Massachusetts Institute of Technology et al., 2021). Remote workers have witnessed an exponential rise in social-engineering attacks where they have been manipulated to open malicious social media links where awareness training can help update on the need to be alert to emerging types of cyber-attacks and to protect their organizations from possible financial, personal, and reputation loss (Hijji & Alam, 2022).

Cloud security awareness can assist the professional in selecting the right cloud service provider and cloud service model, configuring, and managing cloud resources with least privilege, applying encryption, backup, and recovery methods to cloud data and applications, monitoring and auditing cloud activities for any anomalies or suspicious events, and reporting any security incidents or vulnerabilities to the appropriate authorities. When employees consciously or unconsciously engage in risky cybersecurity behaviors, the direct or indirect negative impact from such behaviors is more often disastrous (Ifinedo, 2023). Cloud security awareness can help an organization reduce the risk of cloud security breaches and data loss, improve the performance of cloud operations and projects, increase customer and partner trust and satisfaction, save money on remediation and recovery costs, and reinforce organizational cloud security posture and reputation. Employee negligence and insider breaches sometimes threaten a company's information security efforts (Chen et al. 2012). If public opinion affects the credibility of threat responses, then there is need for an understanding of the opinions of the public on cyber-threats (Leal & Musgrave, 2023). Considering the current skills gap and demand for cybersecurity professionals, an analysis of the current cybersecurity job

requirements would be beneficial to inform higher education and training programs on necessary and required skills to build capacity and competencies for a cybersecurity workforce that meets the qualification demands of the industry (Ramezan, 2023).

Cloud Security Governance

Information security governance has emerged as an essential component of strategic management because of its role in safeguarding critical information assets, and an adequately implemented and compliant governance framework can enable the implementation of and compliance with strategic management directives (Solms et al., 2023). The essence of information security policies as guidelines to specific work tasks or specific technology is in defining acceptable compliant procedures for end users since their noncompliance has emerged as a problem large enough to harm revenue streams, reputation, and trust (Karlsson et al., 2022). The internationally accepted ISO/IEC 27001 standard, which provides common standards for implementing an information security management system has not been widely applied since its publication more than a decade ago (Mirtsch et al., 2021). The UK's Security of Network & Information Systems (NIS Regulations) and Europe's European NIS Directive require individual organizations to be responsible for cybersecurity requirements, but interdependence from connected services utilize components, products, and services from multiple supply chains (Wallis & Dorey, 2023). The EU has developed a cybersecurity policy to govern its online infrastructure and services (Farrand & Carrapico, 2022).

There is need for public–private partnerships to find multifaceted strategies to secure information networks has shaped the fundamentals of cybersecurity approaches in

the past decade. The over reliance on critical infrastructures, the ever-increasing risks of possible cyber-attacks, the possibility of the private sector not being able to meet baseline security requirements without government support and the increasing opinions that cybersecurity is a public good makes it very essential for a public-private partnership in finding the right solutions to secure and safeguard these critical infrastructures (Kianpour et al., 2022). Though there are benefits of migrating to the cloud, including ease of deployment, cost effectiveness, increased performance, and the ability to move quickly and easily, security and compliance challenges abound. Data breaches, system errors, identity and access management problems, and insider threats are some security challenges in the cloud environment that enterprises must address. The critical underlying business issue is the need for effective cloud security governance. Although the research results show that a multifaceted governance structure has effectively achieved collective action when confronted by threat incidents, it is essential to develop a harmonized private/public plan to manage cybersecurity more efficiently as a public good (Kianpour, 2022). Corruption, a societal ill that has hindered adequate institutional quality in the past, threatens institutional governance and policy implementation (Abbas et al., 2022). A cybersecurity response describes how an organization monitor threats, deploys preventative and detective countermeasures, and rapidly reacts to disaster recovery (Jeyaraj& Zadeh, 2022). Solms et al. (2023) stated that the use of information to aid business operations has expanded to its use to gain a competitive advantage, thus it is imperative for organizations when implementing governance practices to include strategic, tactical, and operational activities at all management levels.

Information security policy is one of the most significant formal controls when organizations implement information security, thus, there is a need for automated tools to aid in policy design as most information security managers find policymaking challenging (Rostami et al., 2020). With interconnectivity and availability, the world has become a global village where the governance of cybersecurity risks has emerged as a global issue and not just an issue for corporate board rooms (Huang et al., 2021). Strategic planning, an organized effort to produce the critical decisions and actions to manage, guide and steer an organization or entity in the right direction are needed in the procedures, and tools available to enable IT professional in their daily routines (Alazzawi & Al-Wasiti, 2021). A governance framework can act as a point of reference inbuilt with guidelines, standards, and best practices that form a governance model for cloud security. The government is the entity that promotes cyberspace infrastructure, accepts risks, and safeguards, and promotes the building of a futuristic community that connects people and society at home and globally (Yan, 2022). Effective partnerships of collaboration and cooperation between governments and corporations may seek to develop cyber trade norms and promote responsible corporate commitment to reduce cybersecurity risks to safeguard digital trade, assist in shaping the direction of conflicting cyber norms, and help design strategies to mitigate for transnational cybersecurity risks (Huang et al., 2021). According to Huang et al. (2021), the diversity of governance practices in cybersecurity and the government's mainstream approach to import-related trade policies implementation gives corporations the opportunities to shape cybersecurity governance.

Risk mitigation should be an integral component to ensure the measurement of the effectiveness of enterprise key risk indicators and a reduction in risks over time. Efficient use of resource structures is essential for enterprises to develop and manage cloud security services such as the definition of due process, roles and responsibilities, and procedures for using relevant tools to improve performance efficiency and effectiveness. Persistent monitoring of performance milestones is necessary to measure the enterprise's progress, value, and risk using Key Performance Indicators and Key Risk Indicators to show the attainment of desired benchmarks and key goal indicators over time. A State of Cybersecurity 2021 report by ISACA's research and global survey of cybersecurity professionals across industries stated that 61% of respondents said they had a staff shortage in cybersecurity teams, 44% said it takes 3-6 months to fill cybersecurity positions (ISACA, 2021). Though many contributing factors lead to these shortages, frequently mentioned inhibiting factors to cybersecurity job recruitment are qualification requirements such as education and industry certifications, professional experience, and technical skills (Markow et al., 2019).

Cloud Security Laws and Regulations

Persistence in the release of emerging technologies have caused the problem of ambiguity in the definition of existing cybersecurity problems and regulations and in addition to the fuzziness as to which bureaucratic and legislative bodies have authority has created and continues to create challenges for the formulation of industrial standards and piecemeal policy approaches which in turn require coordination (Lewallen, 2021, p. 13). It is difficult to enact and enforce policy, standards, or ethics because since

technology is constantly evolving, cybersecurity ethical problems are subjected to different social, ethical, and legal guidelines (Dhirani et al., 2023). Cloud service providers and cybersecurity professionals must stay informed of public laws and regulations and be competent to comply with digital security statutes that different countries and regions have enacted to protect and secure their environments. These legislations and standards vary by country (and states), regions, and specific sectors such as the Payment Card Industry Data Security Standard (PCI DSS) which mandates that entities that handle and process credit cards must comply with specific security requirements such as user authentication, encryption and regular software updates, HIPAA, Cloud Security Alliance (CSA), Cloud Controls Matrix and the Federal Risk and Authorization Management Program (FedRAMP) in the US. In response to the market demand for cybersecurity professionals, the National Institute of Standards and Technology (NIST) developed the NICE project, a framework to help educators design credible and up to standard cybersecurity curriculum that train and equip graduates with the capacity, skills, and competencies to meet market job demands. Recent pedagogical research has confirmed the use of the NICE framework to develop the knowledge, skills, and abilities needed in cyber-defense (Armstrong et al., 2020).

Cybersecurity regulations enable IT professionals to engage in information management with an accountable and responsible mindset that should seek to assess and provide solutions to potential threats, reduce the attack surface, secure data, and ensure compliance. The first step is to define the applicable laws and regulations unique to the environment and develop a compliance plan that includes policies and procedures, an

organizational security strategy, implementing adequate security controls, ensuring that all staff members are trained in the relevant regulations, and implementing continuous monitoring procedures to audit and verify that security systems and procedures are compliant.

Laws and Regulations in Effect in the United States

1. The Health Insurance Portability and Accountability Act (HIPAA) was enacted to enforce patient health information protection by agencies that collect and store such information. All health services providers that host patient data in the cloud must be HIPAA compliant.
2. The Gramm-Leach-Bliley Act (GLBA) regulates financial information collection, storage, and management. All service providers that collect or store financial data must be GLBA compliant.
3. The Payment Card Industry Data Security Standard (PCI DSS) protects and enforces compliance on any entity that processes credit card payment data.
4. Executive Order on Improving the Nation's Cybersecurity requires federal agencies to modernize and upgrade their networks to better respond to cybersecurity threats, improve collaboration, and to ease information sharing within and between the public and private sectors.
5. The National Institute of Standards and Technology (NIST Cybersecurity Framework) regulates how governmental agencies generally manage information technology and cybersecurity in particular. Over the years, the agency has drawn a series of guidelines and best practices into a regularly

updated framework that provides public and private organizations with a comprehensive set of best practices for national security defense.

The European Union

General Data Protection Regulation (GDPR) defines the requirements for processing personal data (PII) including how that information is collected and stored in Europe. This legal framework's goal is to combat cybersecurity risks and vulnerabilities while improving the cybersecurity posture of key economic sectors within member states. The downside is that the framework failed to target IoT products (Chiara, 2022).

The United Kingdom

1. Data Protection Act (DPA) defines data processing requirements for organizations that collect, store and process personal data (PII).
2. Cyber Essentials is similar to NIST in the US, but the UK government also requires contractors bidding on government contracts to be Cyber Essentials certified.

Australia

ACSC Essential is the Australian version of Cyber Essentials and the NIST framework that defines mitigation strategies and controls to protect the country from cyber threats.

Cybersecurity Legislation Trends

1. American Data Privacy and Protection Act (ADPPA) is still in its draft form and currently being debated in the US House of Representatives. Though not

yet promulgated into law, the business community must know its eminent effect.

2. California Consumer Privacy Act (CCPA) is a state of California law similar to the American Data Privacy and Protection Act (ADPPA) that seeks to protect the personal information of California residents. It shall require service providers that handle PII and HIPAA to give customers access to and control over their data when enacted.

United Kingdom

1. Data Protection Bill is designed to impose stricter requirements on businesses and is still being debated.
2. Network and Information Systems (NIS) is still being expected to be enacted.

Cloud Authentication and Authorization

The integrity, confidentiality, and authentication of cloud-based information is a significant concern to IT professionals, cloud service providers, and the general private and public user community regarding security. Vahid et al. (2019) stated that large-scale biomedical datasets are exponentially being stored on cloud computing platforms due to the cloud's scalability, adequate backup, high-speed data transfer, and immense storage capacities, but providing secure access is a significant concern. Data storage solutions should have complexity with high-speed processing functionality while delivering needed protections against cyber threats (Emer et al., 2021). Though protocols exist for secure authentication and authorization, data breaches in cloud-stored information have a surged. This surge demands that administrative, physical, and logical security controls

solutions should be designed based on the principles of defense in depth and diversity of defense and least privilege and separation of duties. It should be a careful mixture of deterrent, preventive, corrective, recovery, detective, and compensating controls that align with internal standards to serve the confidentiality, integrity, and availability of stored data (Bederna et al., 2021). Bruzgiene & Jurgilas (2021) stated that information systems have become an increasingly common target for cybercriminals as they seek to exploit known and unknown vulnerabilities for financial or political gains. Authentication is a process that verifies and confirms the identity of an individual or device as the authorized user with granted access rights, where the system requests the user to provide his identity or credentials to prove that he is who he says he is before using the system.

1. Two-factor (2FA) authentication is a protocol to ensure reliability. Bruzgiene & Jurgilas (2021) stated that the user must provide two different forms of credentials to identify and verify whom you say you are such as static login credentials and a token. Villalón-Fonseca (2022) stated that cybersecurity reports have provided evidence of recurrent problems and an increase in their frequency of occurrence, without an efficient strategy to solving them and existing solutions have proven inadequate, thus, managing cloud security needs a new approach from research and development. It is a best practice to develop a workable solution that addresses reliability, safety, resilience, and productivity concerns (Weiss et al., 2022).
2. Role-based access control (RBAC) secures access by assigning user permissions based on the role played within an organization. RBAC offers a

simple approach for IT professionals to manage cloud access as a group rather than the individual permissions approach that has witnessed errors. RBAC role management analyzes users' needs and groups them into roles based on everyday responsibilities. The IT professional then assigns roles and permissions to users depending on assigned tasks, need to know, and the principle of least privilege.

3. Federated identity management (FIM) is a single login multiple access based on a mutual trust agreement between multiple domains are interconnected with functionality to enable users to use the same digital credentials to access related networks within their realm or trust domains such as an organization, business unit, a subsidiary, or a social community. FIM allows each trust domain to maintain its interlinked identity management system. Traditional identity and access management (IAM) systems are focused on enabling enterprise users to access corporate systems.

With medical data distributed across platforms, access to large-scale cloud-stored biomedical data is not secure because existing protocols used to secure authentication and authorization are generally not adopted in bioinformatics and even when used, are challenging to even technologically savvy users (Jalili et al., 2020). The process of managing these pillars of IAM is different for every user base because customers would prefer not to have to remember passwords for every site visited, whereas internal users do not need to access multiple sites as they only access various applications internal to the organization and can use single sign-on (SSO) capabilities (Roy, 2020). What is certain is

that while malicious and emerging technologies beneficial to users, there is an urgent need to address cybersecurity concerns because cyber-threats erode users' trust and significantly hinder the development of new information and communication technology devices and services (Matheu et al., 2020).

Section 2: The Project

Section 2 comprises the purpose, role of the researcher, participant characteristics, research method and design, sampled population, research ethics, data collection methods and techniques, data instruments, data analysis, and reliability and validity measures of this study.

Purpose Statement

I used a qualitative single case study approach to analyze data collected from current information technology security professionals on the practices they use in managing cloud security and reviewed publicly available information. I sought to explore access control strategies that information technology professionals implement to secure and protect data on their cloud infrastructures. To achieve this aim, I conducted one-on-one telephone interviews with practicing cloud security professionals from the contiguous United States who had at least 3 years of experience implementing, securing, and protecting cloud infrastructure using access controls. Insecure cloud infrastructure opens a network to exploitable vulnerabilities that may lead to a breach of the network. Cybersecurity breaches lead to loss of customer trust with damaging material costs and reputational and social impact.

Alharbi et al. (2021) evaluated the impact of security practices and the result of cybersecurity attacks on small enterprises and found that 14.2% of respondents confirmed financial damages to their enterprise due to a cybersecurity breach, 20.5% confirmed that they lost sensitive data due to a cybersecurity breach, 50.3% reported a service restoration time of days or less, and 9.6% reported that it took months to restore service.

Consumer Reports (2022) surveyed 2,103 U.S. adults and found significant loss of trust in consumer cybersecurity and privacy practices over 3 years in a period that also witnessed an exponential increase in consumer online spending by 44% compared to the previous years. A breach can potentially expose PII and financial information and damage brand, corporate reputation, and social trust. When cybercriminals disrupt fueling operations at the gas pump and prevent the everyday citizenry from daily routines or people wake up to find their leaked bank records on the Dark Web, they personally feel and experience firsthand the tangible effect of a cybersecurity breach on their lives (Vijayan, 2023).

The psychological effects and widespread impacts of a data breach include the WannaCry ransomware incident that critically impacted various organizations in 150 countries globally (CISA, 2018). WannaCry disrupted the U.K.'s National Health Service infrastructure in which scheduled operations and services such as surgeries were canceled. WannaCry went beyond disrupting economic activities and maliciously and severely compromised the U.K.'s health care technical system, affected everyday individuals, and made cybersecurity a reality to the everyday citizen (Akbanov & Vassilakis, 2019). WannaCry demonstrated to the local community that exposed vulnerabilities in basic infrastructure could increase anxiety and social distress for the community.

Cyber breaches vary in form and the effect may be wide-ranging or localized and frustrating for the community directly impacted. In 2019, a ransomware attack on a software vendor affected the community of a small Texas town when administrative

services were interrupted and prevented residents from accessing records or pay utility bills (Bleiberg & Tucker, 2021). The cybercriminals demanded $2.5 million to restore services. The current study was intended to identify best practices that may mitigate the increasing number of breaches and better protect a society that has become vulnerable due a convenient reliance on the life-changing role of technology in the global community. Society's reliance on technology mandates the need to build a baseline level of operation from which the consequence of noncompliance can be measured from a minor incident to a catastrophe (Bederna et al., 2021).

Role of the Researcher

It is the researcher's responsibility to collect quality data in an honest and ethical manner when undertaking a study (OXFAM, 2020). A qualitative case study requires the researcher to collect relevant information from multiple sources using archived data, publicly available documentation, observations, and interviews (Yin, 2014). The researcher should be an objective interviewer considering the complex nature of the researcher's role in safeguarding research ethics (Collins & Stockton, 2022). My responsibility as the primary data collection instrument was to collect credible data without bias in selecting the persons to be interviewed, choice of questions, interview environment, or materials. My role as the primary researcher was also to recruit interviewees, interview participants, and collect and analyze publicly available data. I was obligated under the IRB ethical code of conduct to ensure that the research process including research environment, artifacts collected, and participant data were free from any biases that may affect the information collected and analyzed (see Valkenburg et al.,

2020). It is often challenging to avoid bias and personal viewpoints when acting as the primary data collection instrument in participant interviews (Roulston & Shelton, 2015). With more than six years of experience managing cybersecurity risks with specialty in vulnerability management, I have been able to ensure a secure platform and reliably protect information systems on several infrastructures. My background in and knowledge of cybersecurity motivated me to investigate best practices to better protect cloud infrastructure. I made sure that my work experiences and life experiences did not interfere with my judgment and analytical objectivity (see Barrett & Twycross, 2018).

I employed due diligence during the interview process to make my study reliable, credible, and nonbiased by not framing questions in a manner to influence interviewee responses in any one direction (see Federal Deposit Insurance Corporation, 2021). Due diligence helps researchers to foster internal alignment on defined goals and priorities, increase understanding to support more positive and impactful portfolios, and improve communication and strengthen relationships (Brett & Woelfel, 2019). The interview recordings in the current study were transcribed using the NVivo automated transcription service and analyzed thematically. The information had been presented verbatim and was verified to ensure that there was no misinterpretation. I used the Belmont Report's (1979) ethical guidelines and standards designed to protect human subjects in research as my terms of reference in handling human subjects. The Belmont Report, which was first published in the Federal Register in April 1979 by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, sought to address

informed consent, privacy, and anonymity issues and to protect data collected from or about human research participants.

All current participants were provided informed consent forms, and I verbally explained the purpose and intention of the form to them that they were voluntarily participating in the research and could freely opt out at will without prior notice. Participants' personal information such as email and phone numbers were collected for the purpose of interview and interpersonal communication. None of this information was shared with anyone to protect the participants' privacy. Also, I did not used participants' names and personal information in this research report. All information collected from participants was encrypted and securely stored in a locked folder according to the strictures of the IRB (Institutional Review Board, 2024). I used an interview protocol to standardize the interview questions to ensure consistency and repetition among interviews and employed the funnel technique to conduct the interviews by phone (see Dunwoodie et al., 2022). The interview protocol (see Appendix A) also provided guidelines to ensure all interviewees were asked the same questions and received fair treatment. Qualitative interviews provide rich and detailed information to understand individual experiences, but an inexperienced researcher may not be able to adequately perform the interview resulting in the need for a pilot interview to ensure a credible research process (Majid et al., 2017). The pilot interview is used to guide the interview and to ensure reliable data (Shakir & Rahman, 2022).

Participants

The criteria to recruit participants for this study were based on the requirements of the IRB and standards that researchers can use to validate the authenticity of information obtained (see Casteel & Bridier, 2021). I followed recruitment etiquette guidelines to provide respect for individuals being interviewed. I also ensured self-awareness and used values of respect, responsibility, compassion, and cultural sensitivity as guiding principles in the research process. The manner in which a person is approached may affect that individual's willingness to participate and their attitude toward the research (Taherdoost, 2022). The current participants were practicing cloud security professionals who had implemented strategies to secure and to protect data on their cloud infrastructure, who were from the contiguous United States, and who had at least 3 years of experience implementing, securing, and protecting cloud infrastructure using access controls. The participants were surveyed using one-on-one telephone interviews (see Rahman, 2023). The rationale for selecting a pool of cloud security professionals as participants was based on the need to have a knowledgeable and experienced participant base to ensure that the information collected would be reliable and credible and would help improve cybersecurity methods to enable business services to be more secure and to provide the community with a more confident and trusting cloud platform for personal, e-commerce, and social media use (see Inan et al., 2016).

I used a WhatsApp IT professional group to reach out to potential participants who manage cloud infrastructure within the contiguous United States. I solicited voluntary participation from members who provided their contact information such as

email address and phone numbers. I then composed a mailing list of volunteers to whom I sent emails that explained the nature of the research and to obtain their permission to conduct individual telephone recorded interviews. After they individually volunteered to take part in the study, I sent letters of informed consent, which included an outline of the confidentiality and the letter of approval from the IRB and followed up with a phone call to explain their rights including the right to withdraw from the research at will without reason.

The investigation was a telephone recorded interview using the funnel technique to enable me to begin with a broad open-ended question, then gradually introduce narrow follow-up questions that allowed participants to talk from their comfort zones and without fear of body language and physical intimidation. Participants provide more in-depth answers and are more truthful when they feel they are in an environment that is comfortable (Shakir & Rahman, 2022). It is essential to start an interview with a general discussion with the interviewee because it increases trust (Patton, 2015).

Research Method and Design

The qualitative research approach was perceived as the best methodology to explore the strategies that cloud security professionals at U.S. businesses implement to secure access to and protect their cloud infrastructures. A qualitative method is a valid technique to explore current concerns in detail and in depth (Jilcha, 2019). Qualitative research enables the systematic collection, categorization, and analysis of information in any form or format such as conversation (Khanday & Khanam, 2023).

Research Method

Qualitative researchers explore and provide an in-depth view of real-world problems. Compared to the collection of numerical data to assess interventions or recommend treatments, as in the case of quantitative research, the qualitative method is used to investigate real-world problems by sampling participants' experiences, perceptions, and behaviors to answer how and why questions instead of how many or how much. Qualitative researchers use open-ended questions to explore the experiences, attitudes, and patterns of human behavior that are difficult to quantify. The qualitative method also provides interviewees the latitude to freely explain the how, why, or what of their thinking, feeling, and experience at a point in time or event of interest. Qualitative researchers find themes and patterns that are not easily quantified (Tenny et al., 2022).

Information collected from interviews in the current study was organized and separated based on participant metadata, which had been created and linked to an interview file. Archived information was categorized by relevance and time stamp. I collected data from 10 individuals who were employed by 10 different businesses. After the 10th interview, the answers became repetitive and redundant, and I considered that I had reached saturation because there was no new information gained from new interviews.

Research Design

The qualitative research method was appropriate to obtain detailed information from IT professionals using one-on-one open-ended interview questions about their experiences and practices in managing cloud security. The qualitative method was a good

fit for this study because the qualitative method helps researchers gain an understanding of the thoughts and beliefs of participants and recognize the meaning that people attribute to their experiences (Batyashe & Iyamu, 2021). Because my study was not designed to test a hypothesis, the quantitative method was not appropriate for this study. The qualitative method allows researchers to interact with study participants through face-to-face interviews or focus groups in-person, virtually, or via telephone, (Segun, 2022). Case study research is a detailed investigation that requires a substantial period to collect empirical materials from authenticated sources and cases to analyze the context and processes involved in the phenomenon (Chowdhury & Shil, 2021). The case study method is a good fit for information technology research, considering that studying information systems as a discipline has shifted to organizational rather than technical issues (Rashid et al., 2019).

The qualitative method was appropriate for the current study because I sought to collect data from current IT professionals regarding the strategies they use to secure cloud platforms. An organization's information technology strategies on cloud computing and connected cloud networks should have value, visibility, accessibility, dimensions, and suitability (Li et al., 2021). The quantitative method was not feasible because its focus is on the probability and numerical data to intervene or introduce treatments, whereas qualitative researchers explore real-world problems to further understand an issue (Tenny et al., 2022). The current study included multiple case studies to perform research on multiple cloud security professionals employed at two medium-size businesses using one-on-one interviews.

Population and Sampling

The first step in participant sampling was to define participant characteristics. Because the data collection took the form of telephone interviews, the location was broad to include the contiguous United States. Participant selection was based on the participants' ability to provide quality information necessary to answer the research question.

The sample size in qualitative research depends on the researcher who should consider the research question, design, and the nature of the qualitative data to decide on the size to be sampled (Subedi, 2023). I used a non-probability sampling design criterion to ensure that the selected sample could be generalized to the entire cloud cybersecurity population. A non-probability sampling criterion for participant selection has been used in exploratory and qualitative research to help understand a small representative population. Voluntary response sampling was used to seek volunteer participants in this research. Considering that some individuals are more likely than others to volunteer, I considered there could be some bias involved. To mitigate the possibility of bias, a selection criterion of at least three years of participant experience in managing cloud cybersecurity access and located within the United States was employed. People were selected based on the criterion of having had experience in a cloud security work environment in the USA for at least 3 years (Ellis, 2021).

The sampling criterion in qualitative research is not well defined as participant selections rely on the researcher's discretion and the research purpose (Shaheen et al., 2019). I selected my sample from a pool of potential participants who volunteered and

met the selection criterion to qualify to participate. I initially emailed the intent to conduct a sensitive survey to give prospective participants time to decide on whether to volunteer and also provide an opportunity for the prospective participants to reflect on their responses before the survey. A pilot sampling was then carried to access the readiness and enthusiasm of prospective participants with the intent was to familiarize prospective participants with the topic, problem, objectives, and scope of the research with the intent to have an insight into the target population, estimate the response rate and test the quality of the responses. Once I decided the survey would attract enough volunteers with the defined characteristics, I commenced with the interview process. It is essential to exhibit confidence to build trust and self-respect to establish credibility and rapport in recruiting and interviewing research participants (Negrinet al., 2022).

Attaining data saturation is necessary to ensure quality and data validity in research. Data saturation is critical to information collection because it is a measure of how much information is needed to replicate the study and helps to confirm that no new information is gained by interviewing more participants (Hennink & Kaiser, 2022). A qualitative interview research study does not have a fix number of needed participants as information collection may be completed by meeting a data saturation level (Harmon, 2018). In qualitative research, the researcher has the autonomy to select participants with the option to choose from one to twenty samples who vary from the depth of information required and the nature of the study (Subedi, 2021). This study targeted a cloud security professional's social network that enabled access to a large enough volunteer pool to reach data saturation. Using interviews as a survey instrument reached data

saturationthe7th participant (Harmon, 2018). To confirm data saturation, follow-up interviews were also conducted to ascertain that no new information was left out.

Ethical Research

Ethical norms in scientific research are research ethics that help to guide a research project to adhere to ethical norms that promote research aims such as knowledge, truth, and to avoid such error as prohibitions against fake, alter, or mislead research data (Samuel et al., 2019). Ethical norms also promote such social values as trust, accountability and interpersonal relationship environments that safeguard ownership rights, copyright, data sharing policies, and confidentiality rules in peer review. These rules and frameworks help ascertain that that researcher practitioners are accountable and adhere to research conduct, avoid conflicts of interest, and protect human subjects who participate in research. Since most research projects are publicly funded, there is always a need for public support for research because funders are more often attracted to research projects if they are sure of the quality and integrity of the research and also if the research outcome may promote social values and responsibility, public health and safety and if it demonstrably seeks to avoid ethical lapses that may cause significant human harm.

I have endeavored to keep information confidential by securing access to any personal information that I have collected by keeping it safe in a single file. Since the answers were audio recorded, the recorded files were password protected. I also took measures to make the information anonymous to protect interview participants' individual identities though I have reported on aggregated information such as grouped

thematic responses. This study went through Walden University's ethical approval process where my approach in managing ethical concerns and research design, process and procedure was submitted to the Institutional Review Board which approved the research and provided the go ahead. My role as the researcher mandated that I explain my study purpose regarding my ethical responsibility, the role of participants and my responsibility to protect and secure any information collected from interviewees (Benson, & Brand, 2013). I emailed the consent form (Appendix C) to advise the participants of any dangers known or unknown, the participants right that as a volunteer he/she could opt out of the study at will without prior notice, security measures to secure and protect their stored information, duration of storage and when and how the information would be discarded (Kahn, 2014). I started each interview by explaining to the interviewee that to safeguard their information I created separate user accounts for each participant's personal data, encrypted it using Microsoft 365s BitLocker service encryption and used a firewall to secure the computer. Separating user accounts made it easier to protect the data from being affected by other computer activities. Using Windows, I have a single administrator account with strong password strength of 14 characters minimum length, a mixed-case random letters string of numbers and symbols in Microsoft's OneDrive. Though syncing files to personal computers could expose sensitive information to internal threat actors, encrypting computer data and creating independent user accounts can mitigate this threat and protect interview participant information. Robinson (2014) stated that financial incentives may motivate a participant to provide wrong information with the aim of appeasing the researcher. Underhill (2014) stated that monetary or

material compensation could be coercive. I did not offer or provide any incentives to any participant in this study since information from interview volunteers could be influenced by monetary or material rewards.

Data Collection

Instruments

I was the primary information collector where I collected information using interviews and reviewing publicly available information. Qualitative research case study methods obtain evidence from several sources including interviews, participant observations, direct observations, archival records, physical artifacts, and documentation (Ugwu & Eze, 2023). My chosen data collection method as the primary instrument was the interviews method and publicly available information and data. Using qualitative research methodology, I the researcher and the main instrument, has to be a very attentive listener and avoid bias during the interviews (Khanday& Khanam, 2023). Conducting telephone interviews means the interviewer cannot visualize body language in response to interview questions and thus cannot physically influence the responses (Peredaryenko & Krauss, 2013). Since the interviews were not conducted in physical environments, I employed active listening and attention to the participants for any type of responses that enabled me to follow up questions to obtain clarifications. For this study, the questions were preset semi-structured open-ended interview questions. Conducting research using telephone interviews makes it possible to target small niche population groups which is effective in research with professional groups since phone calls enable me to narrow the list of potential participants' relevant volunteers, and difficult to access target population.

More so, niche population groups have in past research studies produced better predictable response rates. Telephone research interviews give clear visibility on the number of contacts available that face to face interviews do not. Telephone interviews also improve respondent validation in that it makes it better to ensure the qualification of each respondent by contacting individuals directly to get their participation and ensure each individual meets defined criteria. Telephone interview research studies also provide better qualitative feedback that is difficult to capture through one-way communication research methods such as online surveys as participants feel included as active participants. An inclusive research approach empowers participants to participate in knowledge creation which builds trust and validates the research results (Verhage et al., 2024). Open-ended questions and qualitative data collection enabled me to delve beyond an interview's top-of-mind recall and ask follow-up questions to get a better understanding of their answers and more elaboration for deeper insights, according to Jason Anderson, Sr. Fieldwork Manager at The Farnsworth Group. In online surveys, if a question is poorly worded, or a participant does not fully understand the question, an opportunity is missed to get real-time follow-up to provide further explanation or clarity. Telephone person-to-person conversations are more engaging and the interviewer control the data-collection process to ensure the collection of higher-quality data and to better explore the ideas that cloud cybersecurity professionals have put in place to reach a point of securing information on the cloud infrastructure.

Collection, analysis and use of open-source information that is publicly available and legally accessible from organizations, governments, businesses, and non-

governmental organizations was very useful for a wide range of topics such as security threats, market research, and competitive intelligence in this research. Cyberattacks, competitor's information, industry trends, and consumer behavior research from a variety of organizations and individuals can be used to inform business strategy and decision-making on social media use trends, public opinion on cybersecurity threads, and the effect of cyber threads on economic indicators. Publicly available information for this has been gathered from a variety of sources, including social media, news articles, commercial databases, government reports, industry releases and academic papers. This approach has made it more cost-effective than alternative forms of collection, such as human intelligence or signal intelligence and does not require specialized equipment or person accuracy and reliability. I have been able to collect this information manually by searching for and reviewing sources. I then processed the information to remove duplicates, irrelevant or inaccurate data filtering and categorizing the information based on relevance and importance. The processed information was then analyzed to identify trends, patterns, and relationships using Excel analyzing feature.

Member checking is a participant or respondent validation technique used in establishing results credibility. During member checking results are reviewed with participants to check for accuracy and to confirm that the information obtained is in sync with their experiences. The goal of member checking is to correct errors by giving participants the opportunity to remove or add information as needed and to provide credibility and trustworthiness to the data (McKim, 2023). Interview information was further validated for reliability using member checking to confirm or correct information

obtained from interview for accuracy and establish trust (Candela, 2019). Through member checking, I used follow-up interviews with participants to review the previously obtained information to confirm with participants and to ensure that my interview transcriptions were correct. Member checking provided an opportunity for participants to review and reflect on their previous answers and to offer corrections or new insights. Early member checking helps eliminate the possibility of misrepresentation and enables the researcher to have accurate data to analyze during the data analysis process (Candela, 2019).

Data Collection Technique

The qualitative case study method research collects evidence from six sources interviews, participant observations, direct observations, archival records, physical artifacts, and documentation (Ugwu & Eze, 2023). I began the research by fulfilling the conditions of the IRB. After the IRB approval, I contacted a social network pool of cloud cybersecurity professionals. I sent an email to all members of the social network explaining that I was seeking to recruit volunteers for a research study. The email explained the purpose of the research, the role and responsibilities of participants and my role and responsibilities as the researcher. I initially published the intent to conduct a sensitive survey to give prospective participants time to decide on whether to volunteer and also provide an opportunity for the prospective participants to reflect on their responses before the survey. I conducted a pilot sampling to access the readiness and enthusiasm of prospective participants and to familiarize prospective participants with the topic, problem, objectives, and scope of the research, have an insight into the target

population, estimate the response rate and test the quality of the responses. Once I decided the survey would attract enough volunteers with the defined characteristics, I commenced with the interview process. For this study, the questions were preset semi-structured open-ended interview questions. Once I selected and compiled a list of volunteers including their names, phone numbers and email addresses, I proceeded to schedule one on one telephone interviews individually (Lindheim, 2022). I emailed consent forms (Appendix C) to them individually explaining the study and again informed of their right to withdraw from the study at any time without reason or advance notice. I also sent reminder emails or text messages depending on their preferences. At the scheduled time I called the participant and began each interview with a general conversation to ease the environment. I conducted each interview within an average of 20 minutes. I asked 9 semi-structured questions and follow up questions where necessary. Each question centered on or was related to the participant's experience and issues encountered when managing cloud security. All interviews were audio recorded using my mobile phone, transferred to my desktop computer and transcript using Excel software (Elhami & Khoshnevisan, 2022). I then reviewed the transcripts, notes taken during the interview and the recordings for accuracy and clarity and resolved any conflicting information. I used member checking as follow-up to further clarify and ascertain the credibility of information and the collection techniques (McKim, 2023). The member checking follow-ups provided participants the opportunity to correct, change or add information. It also enabled me to reach data saturation (Hennink & Kaiser, 2022).

I collected publicly available information from a variety of sources, including social media, news articles, commercial databases, government reports, industry releases and academic papers. I manually collect this information by searching and reviewing several relevant sources. Publicly available information was gathered from a variety of sources, including social media, news articles, commercial databases, government reports, industry releases and academic papers. I then processed the information to remove duplicates, irrelevant or inaccurate data filtering and thematically categorized the information based on relevance and importance. I then analyzed the information to identify trends, patterns, and relationships using Excel analyzing feature.

Data Organization Techniques

Information management in research is very essential as it provides a safe and coherent approach to research and also helps to locate artifacts more easily and securely control access to confidential information. I used multiple methods both electronic and manual to store and organize my information in the course of this research study comprising Zotero reference management software to manage bibliographic data and related research materials such as PDF and ePUB files, Microsoft Excel, Microsoft Word, NVivo's transcription tool to transcribe and analyzes audio files from recorded phone interviews, reflective journals, research logs, research trackers, and labeling systems (Patel, 2020). Participant's information and recordings were individually separated and stored personalized encrypted and coded folders on personal computer to preserve identity and confidentiality of recorded information (Kapiszewski & Karcher, 2021). I used reflective journals throughout the research process as a written record of my

research including what I did, thought, and felt while analyzing the data and the rationale behind those thoughts. Self-reflective journals help in information analysis to reflectively examine personal assumptions and research goals and to clarify individual belief systems and subjectivities (Brailas, et al., 2023). Reflective journals are a strategy that helped me acknowledge the values and experiences of the researchers and research that I consulted rather than attempting to control their values through methods such as talking about the presuppositions, experiences, and actions and rationales behind them.

Data Analysis Technique

The qualitative data analysis technique that I used included unique identifiers as themes. As a data analyst I used recorded telephone interviews and document reviews and artifacts to inductively investigate the data to look for patterns and to develop a theory to explain the patterns in data. Two main qualitative data analysis techniques used by data analysts are content analysis and discourse analysis. Another popular method is narrative analysis, which focuses on stories and experiences shared by a study's participants (Crabtree & Miller, 2023). I used content analysis to identify patterns in the recorded interviews that indicate the purpose, messages, and effect of the content. I first identified the data sources from books, newspapers, government releases industry specific standards and social media. I then identified a criterion to determine what will make a particular text relevant to the study such as a specific topic on cloud security, a related event and a specified date range or geographic location. I then developed a coding system for the data. Because qualitative data is not numerical, there was need for me to codify the data in preparation for measurement. I designed a set of codes to categorize the

data and applied it to specific texts for data examination (Linneberg, & Korsgaard, 2019). I used the NVivo software to look for patterns and correlations in the data to interpret results and make conclusions. Considering that a message is not always what it seems, the ability to determine underlying messages in communication is essential. Since a piece of communication can have an indirect or underlying message, it can be interpreted differently by different by diverse individuals and potentially lead to a wrong conclusion. This stage of data analysis helped provide an understanding of the social and cultural context of the interview conversations. Considering that an aim of this research was to investigate the social context of IT professional's experiences and how they used these experiences to achieve their aims such as building trust. Using discourse analysis techniques in verbal and nonverbal cues, the way a speaker pauses on a particular word or phrase may provide insights into the speaker's intent or attitude toward a particular issue or event (Mogashoa, 2014). Discourse analysis helped me to interpret the true meaning and intent of the IT professional in the interviews and to clarify misunderstandings such as an analysis of transcripts of the conversations could reveal whether the interviewee truly understood a question, differentiate whether the content of publicly available materials was fact, fiction, or propaganda (Suciu, 2023). It was very essential for me to define the research question to determine the aim of the investigation and provide a clear purpose to select the content types of the materials used in my investigation such as what publicly available information to collect and whom and how to conduct interviews and to analyze the content for words, phrases, sentences, and structure to understand patterns in the participant's attitudes, intent and reaction. For this qualitative multiple case study, a

triangulation method was used to increase validity and reliability so that a flaw in one data source would be counterbalance by strength in the other source to avoid flaws in data collected (Bans-Akutey, & Tiimub, 2021).

Reliability and Validity

Qualitative researchers are required to articulate evidence of primary criteria to ensure the trustworthiness of the study's findings (Birt et al., 2016). A research report is only valuable when there is a literary warrant that links the research question to research results to support the claim that captures the readers' trust. It is crucial for the researcher to ascertain that the data collected and used is obtained from valid, reliable and authenticated sources. It was essential to me as the researcher to take necessary steps to ensure that the data that I collected was both valid and reliable. Considering that a research project seeks to explore the unknown to increase knowledge on a given topic, it is critical to undertake a research study void of any fabrication, false analysis, deception or any falsification of data (Christensen et al., 2011).

Reliability

During this research study I took data reliability into serious consideration from the very beginning of research. Reliability helps to ensure that the research approach is true and that the research can be replicated (Babbie, 2010). Reliability ascertains that the research process is consistent with the topic under study from the research question to type and method of data to be collected and intended data analyzes technique. Reliability in a research study has to ensure that the research method is consistent (Svensson & Doumas, 2013). Adequate documentation of research information helps to ensure

repeatability of collected data (Turgut, 2014). Reliability was established by ensuring consistency of the processes because the same interview questions were used throughout the research process and using publicly available information implies that the information has been publicly critiqued and vetted (Chauvette, 2019).

Validity

The researcher must afford adequate effort to provide validity assurance necessary in qualitative research. The researcher must adequately prove the scientific nature of the research to knowledgeably understand the phenomena being studied (Hayashi Jr. et al., 2019). According to Leung (2015) validity in qualitative research refers to the relevance of tools, procedures, and data collected that can adequately lead the research question to achieve the desired outcome, whether the methodology chosen can adequately answer the research question, whether the research design is valid for the methodology, whether the sampling and data analysis is adequate, and the results and conclusions align with the sample and context.

Trustworthiness aligns with validity when information is obtained from trusted sources. Harmon (2018) used member checks to validate interview responses to confirm or correct transcript information in follow-up sessions. I used member checking to ensure that the participants reviewed their previous answers that I transcript and provided each participant the opportunity to make corrections where necessary to increase data validity. I have also ensured validity using triangulation to obtain data from multiple sources from publicly available information on cloud cybersecurity and one-on-one interviews (Rice &Bailon, 2023). This study also observed research ethics by obtaining IRB approval.

The credibility of data was assured by conducting interviews from multiple perspectives to ensure data appropriateness. This was achieved through data triangulation, participant validation through member checks and rigorous data collation techniques so that the data collected was an accurate representation of the phenomenon under study. Credibility in research ensures that the data is correct and that the participant's experiences as narrated in the findings are in congruent reality (Stahl & King, 2020). This criterion was achieved using member checking as participants had the opportunity to verify and confirm or correct the information transcripts and also as a strategy that established and sustained interpersonal communication, built trust and collective reflection between the participant and myself (Nyirenda et al., 2020). Since the interviews were recorded, the recordings were preserved for ready reference.

Dependability

Dependability was achieved by using multiple forms of data obtained from publicly available data on cloud cybersecurity and data triangulation to comparatively review data collected from publicly available sources interview transcripts to further ascertain validity. Data Integrity refers to how consistent, complete, reliable, accurate and trustworthy collected data is managed in its life cycle which is an essential standard for effective academic research that demands quality. Research data that lacks integrity may seriously affect the quality of records and evidence, results, and conclusions. The researcher is mandated with the responsibility and duty to implement and to ensure that adequate data governance practices and integrity is maintained (Pharmaceutical Inspection Convention, 2021).

Triangulation is increasingly used by researchers to generate and test theories to ensure that the results are reliable, credible, and valid (Noble &Heale, 2019). Triangulation in some cases use mixed methods to explain how the researcher used multiple approaches to extract valuable information and to critically analyze the study's data to ensure validity and credibility (Bans-Akutey & Tiimub, 2021). I separated each participant's interview answers into segmented, encrypted, and locked folders on personal computer to guard against data contamination. Each participant's information was assigned a unique code. I analyzed data using NVivo software and kept detailed process notes in a journal format to guide as referral and follow-up where and when necessary. The trustworthiness of data is the core of quality in qualitative research and the researcher's neutrality in data evaluation incorporating sampling and data analysis most be dependable (Stahl & King, 2020). Member checking was used to increase dependability and creditability because it allowed participants to verify and confirm or correct interview transcripts to validate data credibility and saturation (McKim, 2023). Mwita (2022) in a review of the literature on qualitative approaches determined that five factors consisting of coding system, sample size and themes, resourcefulness of participants, research method, and time spent on data collection sessions influence data saturation and concluded that it necessary for researchers to approach qualitative studies using multiple factors that may affect data saturation to increase the validity.

Transferability

Transferability refers to the extent to which the results and conclusion can be transferred to other cybersecurity environments or seeks to determine if the same findings

can be replicated with participants in a different context, setting or geographic region (Megheirkouni & Moir, 2023). Transferability was achieved by interviewing participants from multiple and devise firms and by utilizing a broad web of publicly available resources on the topic to capture rich and knowledgeable information which can be applied to the entire cybersecurity spectrum. Transferability may consider such sampling factors as the number of respondents, participant characteristics and the time and geographic location of data collected (Johnson et al., 2020). I used purposeful sampling method to enhance transferability (Madondo, 2021). All data and information collected from participants and publicly available materials can be vetted publicly for accuracy to provide credibility. The data was recorded and securely preserved so that it can be used by other researchers to replicate this study or conduct another research.

Confirmability

Confirmability was assured when the data collected was checked and rechecked during data collection and analysis to ensure repeatability of the findings by others. Transferability in qualitative research seeks to align the study with as much objective reality as possible (Stahl & King, 2020). I used a technique called audit trail in the form of a reflective journal to document the research process and codes and patterns to uniquely identify individual participants in the analyses. Confirmability was also ensured using triangulation and member checking of the data to mitigate personal bias. To ensure confirmability, participants were allowed to review interview transcripts to confirm, correct or change any information. Confirmability was also ensured using reflective journals to document all processes from data collection, document analysis to conclusion.

By allowing the participants to confirm their interview transcripts and by using publicly available information that can easily be fact checked, credibility was established from the participant's viewpoint, validation methods, and information sources (Megheirkouni & Moir, 2023). Using information that can easily be fact checked adds validity to the collected data.

Section 3: Application to Professional Practice and Implications for Change

The goal of this study was to investigate strategies that cloud cybersecurity professionals implement to secure access to their cloud infrastructures. This third and final section presents the findings gleaned from professional cybersecurity individuals and publicly available information. The relevance and need to protect and secure information stored in the cloud is not only a critical national security issue but also of immense importance to the many internet users who daily expose their personal and private information to cybercriminals (Alazzawi &Al-Wasiti, 2021). My intention was to use deductive reasoning to present best practices in cloud cybersecurity that cloud security providers can implement to improve, secure, and protect their cloud infrastructure and environments. The information that led me to these best practices and standards was sourced from credible and reliable individuals and authoritative publications (see Sobel & Vetter, 2022). The findings indicated that inadequate configuration methods, lack of due diligence, business competitors fighting to have competitive advantage, cybercriminals' profit and revenge motivation, and nation state actors are the main reasons behind the multitude of breaches occurring daily.

Overview of the Study

It is essential to keep security processes simple to benefit and ease the burden on the common user who in most cases is far from being information technology savvy. Considering the enormous and irreversible cost of a security breach to a business, the society, and the individual, security strategy complexity becomes a sine qua non (Krutilla et al., 2021). User authentication is a necessary first step because it provides users with

access to the cloud infrastructure. Role-based user authentication provides access based on need to know as a pivotal initial security point (Bruzgiene & Jurgilas, 2021). Internal threats resulting from improperly granted access rights, negligent or disgruntled employees, misconfigurations and inadequate controls, and lack of continuous monitoring are some of the key issues that need urgent attention. Proper and adequate management of identity and access issues in the cloud is a major challenge for service providers to resolve (Partida et al., 2021). This may be mitigated with strength-based authorization and authentication policies that can safeguard not only the information stored on the cloud but its entire network.

Presentation of the Findings

I sought to answer the following research question: What strategies are used by cloud security professionals to implement secure access methods to protect data on the cloud infrastructure? Using coding and thematic analysis, I was able to identify primary themes: (a) data protection, (b) authentication and authorization, (c) input and output handling, (d) error handling and logging, (e) configuration and operations, (f) session management, and (g) access control methods (see Thompson, 2022). The UTAUT was used to investigate technology acceptance with performance expectancy, effort expectancy, social influence, and facilitating conditions as predictor variables based on the interview transcripts and publicly obtained information to determine whether these variables were significant. The UTAUT had been used in previous studies to determine a person's intention to use technology and to show the associated relationships between effort expectancy, performance expectancy, behavioral intention, facilitating conditions,

and social influence (Popova & Zagitova, 2022). I analyzed the participants' responses and publicly available documents to determine the influences of effort expectancy, performance expectancy, behavioral intention, facilitating conditions, and social influence on information technology professionals' cybersecurity practices.

The first interview question was the following: How much experience do you have managing cloud security in general and cloud identity and access management in particular? The study a participant's characteristics is essential because the human factor in terms of human error, human behavior, human performance, and decision-making capability. SANS Institute (2024) warned that a review of cybersecurity reports from CrowdStrike, Verizon Data Breach Incident Report, Gartner, and Thales all confirmed that human factor remains the weakest link and top driver in cloud breaches because information technology administrators and developers are not only major targets but have been found to make mistakes given the complex cloud environment. Hewavitharana et al. (2021) reviewed 55 journal articles to determine whether human behaviors affect digital transformation in the construction industry using the UTAUT model and concluded that there is a need for further studies on the role of human factors and management in digital transformation and successful cloud security practice. Bayaga and du Plessis (2023) surveyed 264 respondents from one university in South Africa to correlate the behavioral intention of tertiary staff with existing findings using the UTAUT model and found that performance expectancy, effort expectancy, attitude toward using technology, social influence, self-efficacy, anxiety, and facilitating conditions influence behavioral intention and have predictive validity.

The characteristics of the information technology professionals interviewed were varied and in diverse categories. Some worked in information technology operations where they managed day-to-day activities such as security testing, assets management, and tech support such as laptop, desktop, phone system, and server. Some were in information technology governance managing compliance and audits processes that an organization needs to ensure that systems are operating effectively and according to regulations. Some respondents were engaged in cloud network and configuration management activities that ensure a secure and resilient infrastructure. Participants generally consisted of information technology professionals who build, test, install, repair, and maintain hardware and software within their organizations with some of them in-house and the rest working for service providers that range from small to medium-size businesses. Six of the information technology professionals interviewed had a background in computer science or information technology, one was home grown, and three transferred from unrelated fields. All information technology professionals interviewed had benefited from continuous education and had completed certification programs because of the evolving nature of technology and systems. All ten information technology professionals who participated had been managing cloud security for an average of 4.1 years ranging from 3 to 7 years.

Chapman and Reithel (2021) used the UTAUT to survey135 information technology managers at U.S. public colleges and universities to determine perceptions of their cybersecurity readiness including previous cybersecurity experience, their use of network activity monitoring behaviors, the extent of their involvement to exercise

physical control over computer resources, and the degree to which implemented preventative controls. Findings indicated no statistically significant direct effect on level of previous cybersecurity experience and perceived readiness to detect a cyberattack. This finding can be attributed to the continuing challenges in detecting extant cybersecurity threats.

The next interview question was the following: What challenges with specific incidents have you experienced since you migrated to the cloud? From the interviews, the challenges were not the same for everyone because their environments were unique and diverse. More than half of the interviewees said configuration and operation issues were their major challenges, a few said input and output handling was challenging, and all mentioned data protection as a key challenge. Configuration management was mentioned multiple times in the documents reviewed. The documents that I reviewed all established a need for a robust change management process that tests new releases before deployment and continuously during operations. A critical method to achieve this is to automate application deployment to ensure a consistent, repeatable work environment. Public laws and industry-wide standards mandate integrating appropriate security countermeasures into the design and architecture with continuing risk assessment by security professionals to identify and preempt risks. This should include security-focused code reviews using automated tools to identify security bugs to guard against SQL injection and Cross-Site Scripting. It is also essential to set policies that develop and implement an incident response process, harden the infrastructure, educate personnel on security awareness, and ensure consistent testing and continuous monitoring.

Input and Output Handling: Most professionals interviewed said they use a whitelist blacklist policy to manage access control in the cloud because all user input fields are configured to validate the input content. The documents reviewed indicated that using tokens can prevent forged requests by embedding a unique random value of each request into the HTML to avoid intrusion from unknown to third parties. The evidence also indicated a need for uploaded files from users to be validated for file size, file type, file contents, and source of input to make it impossible to override the file destination path. Findings also indicated using the content-security-policy header with configured security policy to secure the application and mitigate the risk of known exploited web security flaws such as cross-site scripting and click-jacking.

Data Protection: Both the documents reviewed and the information technology professionals interviewed affirmed that using secure protocols such as HTTPS is a sine qua non for all network data transfers. Data encryption helps to protect the confidentiality and integrity of data at rest and in transit such as the use of robust TLS configurations. Data in transit must be configured to support recent versions of TLS, the most robust cipher suites for Perfect Forward Secrecy, such as Qualys SSL Labs and testssl.sh, SSLyze, sslscan. Popular user access methods such as usernames and passwords should use strong, iterative, salted hash, and secured with protected and robust algorithms such as SHA-512 hashing, bcrypt, or PBKDF2 techniques. Stored keys or credentials must be protected and accessed based on a need-to-know policy. Most information technology professionals interviewed reported that leveraging a secret/key management solution such as Azure Key Vault, Hardware Security Modules (HSM), GCP Cloud Key Management,

AWS KMS and certificates from a reputable certificate authority is good practice. Browser data caching and login forms that are sensitive input fields should be turned off so that the auto complete attribute in the HTML form can instruct the browser not to cache the credentials. The interviews also indicated that reducing the quantity and use of sensitive stored data should be highly encouraged.

Error Handling and Logging: This theme was mentioned as a pivotal best practice in securing a cloud infrastructure. Though only half of those interviewed discussed error handling, peer-vetted materials from publicly available materials consulted for this study emphasized that it is essential for network protection. The SANS Institute (2024) insisted that details in error messages should avoid any situation in which the application's internal state is revealed, such as file system path and stack information or authentication errors that could reveal the existence of the username. Considering the many languages and frameworks used in developing web applications, it is essential to configure the system to handle unforeseen errors and return controlled output to the user without letting an unhandled exception occur. Because logs can be used to predict signature attacks and attacks in progress, it is critical to log any authentication and session management activities as well as all input validation failures and security-related events such as user privilege level changes and access to sensitive data that is critical to corporations or meets regulatory requirements such as HIPAA, PCI, or SOX in encrypted form. All logs must be securely stored and retained to avoid loss of information or tampering. Xue et al. (2024) conducted a systematic reviewed of 162 SSCI/SCI-E articles from 2008 to 2022 to analyze the application of the UTAUT model with a focus on higher education students

from Asia and North America and found that performance expectancy has the strongest influence on behavioral intention.

Evidence from empirical research has shown that human factors remain crucial in cloud security because information technology professionals must implement and comply with established rules and regulations, provide user awareness and education about potential risks, and perform continuous monitoring and audits. Taiwo and Downe (2013) conducted a meta-analysis of 37 empirical studies based on the UTAUT model and found an overall strong relationship between performance expectancy and behavioral intention and weak relationships between effort expectation, social influence, and behavioral intention. Though cloud security threats can emerge from anywhere, information technology professionals are guided by many cloud security standards, but understanding and navigating these cloud security controls is complex and may overwhelm a professional. The cloud security professional must understand and build capacity competency skills in implementing the proper cloud security standards that address the unique critical business mission of the entity. Matar and Al Malahmeh (2020) used the UTAUT model in a survey of five Jordanian university information technology professionals to identify factors that affect the behavioral intentions to adopt new technologies and concluded from the results that there was high behavioral intention to use cloud services and solutions within their workplace, which were moderated by facilitating conditions such as the level of support from management.

The next interview question was the following: How do you protect your system against unauthorized access and what factors do you consider when developing strategies

and policies to manage unauthorized access? This study's aim was to identify strategies to implement and manage cloud access control. Access control was a critical finding. All participants to whom I posed this question mentioned the need to adopt the least privilege policy based on a mandatory access control standard. A thorough review of the documents also indicated a need for all access control policy decisions to use the principle of least privilege as a baseline. Williams et al. (2015) conducted a systematic review of 174 articles that used the UTAUT model and concluded that the most researched topic areas were general purpose systems and specialized business systems, and that performance expectancy and behavioral intention were the best predictor variables. These baselines include but are not limited to performing access control on static resources, ensuring that static application resources are incorporated into the access control system including cloud-based static resources, using the same access control logic on the static resources where possible, and not using invalidated resources. It is a best practice to conduct adequate authentication checks before linking the user to a given resource because an invalidated forward and subsequent resource use can result in server-side request forgery issues.

An inherent aspect of cybersecurity is to manage incidents by implementing strategies that are effective and produce a secured response. Since cybersecurity strategy policies are based on decisions influenced by inherent characteristics because the consequences of security strategies choices are often not certain and laced with action bias that result in ill rational behaviors, the need for mitigation is often inhibited by lags and latency until effects are felt. Performance Expectancy (PE) therefore measures an IT

professional's belief in the extent to which a piece of technology can help attain gains in job performance (Venkatesh et al., 2003). Valerie et al. (2021) used the UTAUT2 framework to study the acceptance of the Bukalapak e-commerce system, while Dwivedi et al. (2017) tested the revised model using data from 1600 observations involving 21 relationships from 162 research studies on IS/IT acceptance and use and concluded that the model was meaningful for understanding IS/IT acceptance and usage. The exponential increase in the value of e-commerce influenced by innovative advances in digital technologies such as cloud computing has helped to drive the adoption and use of emerging technologies by organizations (Verhoef et al., 2021). Considering the impact of technology adoption on an organization and associated effects on performance and cost-revenue values, the gap between technology utilization-acceptance continues to be a major concern (Marikyan & Papagiannidis, 2023).

The next interview question was the following: What techniques have you found most effective in designing and implementing adequate access control and why does this technique impact and give you a competitive edge in the industry? User authentication is the most emphasized strategy mentioned in the access control policy. Password reset systems were considered the weakest link in user access control methods. Since these systems are designed to have users answer personal questions to authenticate their identity, these questions must be hard to guess to avoid a brute-force attack. An authentication system must be configured to not communicate any information about whether the account is valid to prevent username harvesting. Account lockout to prevent brute-force attacks functionality should be designed not to disclose sensitive information

in error messages that indicate that a user ID is valid. Thus, a message saying that the corresponding password is incorrect would confirm to the attacker that the account does exist.

Since the cloud infrastructure requires network access functionality, authentication through application-provided credentials is necessary, but securely storing and safely protecting these credentials is a major security risk that can be addressed by secrets management solutions that provide on-demand credentials functionality without the risk of storing them on disk such as AWS Secrets Manager and Hashicorp Vault. Authentication can best be implemented using the least privilege policy, but human behavior remains key to effective and successful implementation. Dwivedi et al. (2023) conducted a meta-analysis of 1600 observations from 162 studies on IS/IT acceptance and use and 21 coded relationships and concluded that attitude was strongly associated with behavioral intentions and usage behaviors.

The next interview question was the following: What are the challenges relative to the strategies used in designing and implementing access control policies, how do you handle user access complaints, what are the most common access complaints you receive from users and what types of training do you offer to staff and system users on access control best practices, especially password complexity? Adequate security policy was a recurrent theme that frequently appeared from the data analysis. Adequately implementing secure security policies and ensuring compliance was mentioned and recommended as the proper method to address and better protect the network. Cybersecurity professionals' task with designing and implementing varying security

policy requirements within their environments must adhere to proper system configuration standards and access controls such as password complexity. Cybersecurity professionals must implement security policies to secure and protect enterprise systems and guest networks from increasingly sophisticated cyber-attacks and costly breaches. Security policies are designed to protect assets from imminent threats that threaten a firm's reputation and user trust (Solms, 2023). This research aims to provide knowledge and understanding on the need and the how to design strength-based security policies to benefit both the company and the user. Most participants interviewed were motivated and believed that they were contributing to knowledge that they felt made them change agents in the global war against cybercrime. The need to implement secure security policies was echoed by all interview participants and documents reviewed. Documents from the US government's NIST standards, the European Union and industry specific standards such as SANS framework all addressed this theme in varying degrees. All documents reviewed stressed how critical it is to implement a strength-based security policy that is integral to effective and secure asset protection.

The next interview question was the following: How does the general shortage of cloud security professionals or experts affect your business model in terms of management position on training and grooming in-house staff to fill these vacancies, time management and how would you prioritize if several challenges came up simultaneously (upgrade/patch management deadlines, zero-day incidents, corporate meetings, teaching commitments)? The respondents were all unanimous that there is significant IT talent shortage in the US. Thus, their organizations have had to rethink their hiring and

retention strategies. A MIT Technology Review Insights (2024) survey reported that 64% of IT executive respondents opined that most IT job candidates do not have the necessary competencies, skills or experience. The report also stated that a further 56% of IT executive respondents felt the overall shortage of candidates was a significant concern. The year 2030 may witness an expected global talent shortage of about 85.2 million in the ICT industry (MIT Technology Review Insights, 2024). Technological and digital advancement resulted in the rise and use of robotic process automation (RPA) solutions that effectively replaced low-to-mid-level skilled workers. Though this approach enabled businesses to achieve cost effectiveness and improved efficiency, it triggered an exponential demand for a new a set of skilled workers to manage these new technologies while the education system has not been able keep pace and produce enough graduates with the necessary capacity building competencies and skills. More so, the COVID pandemic triggered an exponential switch to remote work which in turn created additional demand for skilled IT professionals as businesses went digital, changed their development approaches and strategies to data security. The consequences of talent shortage are enormous and make significant barriers to the adoption of 64% of emerging technologies. These barriers include slowed down growth and development, unrealized revenues and increased costs and hiring efforts. According to MIT Technology Review Insights (2024), it is expected that by 2030, the talent shortage may be about $8.5 trillion in unrealized annual revenues. The report estimated IT talent shortage could cause the US to lose $145 billion worth of revenue annually. A Manpower Group report on US skills

shortage statistics stated that 69% of businesses were not able to fill positions in 2020 (ManpowerGroup, 2023).

The next interview question was the following: Is funding a barrier to hiring and retaining talented and experienced cyber engineers if so, how do you intend to solve this problem and how do you convince management to fund your project instead of other departmental priorities? What additional information about your experiences protecting your system against unauthorized access would you like to share, what would you do differently if you were starting your job again today, what do you see yourself doing in ten years and what are your professional goals in the next five to ten years? Another critical issue in cloud access control is the management of user sessions. One IT professional opined that from his experience, session identifiers generate secure random functions of adequate length and strength to be resilient against predator analysis and prediction. Design and configuration must authenticate users accessing an application by regenerating session tokens and when there are functionality changes such as encryption status and user privilege level changes. Session management configuration must also enforce idle and absolute session timeout, terminate a session if there is any indication of tampering and cookie domain, path and attributes must be secure and set correctly, session logout must be invalidated immediately, and each page should be designed with a logout button. NIST SP-53 and SANS provide standards that recommend secure baselines that if implemented void of human factors may effectively secure a network. Tanantong & Wongras (2024) used the UTAUT model survey to explore 364 HR experts on factors that influence users' intention to adopt AI in recruitment and concluded that

perceived value, perceived autonomy, effort expectancy, and facilitating conditions, significantly impact the intention to adopt AI for recruitment but though social influence and trust were determined to not have a direct influence on intention, social influence was found to directly affect perceived value. Ayaz & Yanartaş (2020) used the UTAUT model to survey higher education employees to determine factors affecting the adoption and use of EDMS in the University and concluded that 61% of the intention to use EDMS was positively influenced by performance expectancy and social influence factors but not effort expectancy factor.

Zamberlan &Watanabe (2020) used the UTAUT model to determine the use and acceptance of information technology as a decision support tool in a public educational institution and concluded that in the adoption of IT as a decision support system, the moderating variables of gender, age, and experience were statistically not significant but the managers accepted the tool as essential for developing activities with ease of use and high performance expectancy as key variables in the adoption of new technology. Popova & Zagulova (2022) used a questionnaire based on the UTAUT model constructs of personal information (age, gender, education) to survey the efficiency of using technologies, the efforts needed to use the technologies, general attitude to using technology, social impact on the person regarding the use of technologies, factors facilitating the usage of technologies, self-efficiency and anxiety about using technologies and concluded that facilitating conditions remain a major determination because it is very essential to enable appropriate conditions for users such as user awareness education.

The Sarbanes-Oxley law of 2002is defined by 15 US Code Chapter 98, which requires public companies to prove their cybersecurity credentials by managing risk through internal controls processes that make complete, accurate, financial, and operational information for informed decision-making and reporting. This legislation and regulation mandates companies to use due diligence to meet their fiduciary duty by providing financial statements that are accurate or face penalties. Penalties bind a CEO or CFO found liable with fines that may not exceed $5 million and imprisonment with a maximum sentence of 20 years.

The SEC Regulation S-P, the Privacy of Consumer Financial Information and Safeguarding Personal Information under 17 CFR Part 248, Subpart A SEC rule 30 is a federal law that regulates information security and mandates institutions to implement defined baseline cybersecurity measures such as zero trust. This rule mandates US and foreign securities and commodity firms to adopt and implement baseline security policies that meaningfully secure and protect client information and data at rest and in transit against unauthorized access. Noncompliance can result in civil fines for up to $1,098,190 or triple the monetary gain. This law is critical to cloud cybersecurity because it holds securities and commodities firms accountable in their fiduciary duty to use due diligence to secure and to protect the integrity and confidentiality of sensitive customer data and information against potential internal and external threats, hazards and unlawful use.

Gramm-Leach-Bliley Act (GLBA) under 15 US Code Subchapter 1is a federal security and privacy law that regulates information security and mandates financial institutions and related organizations to implement baseline controls designed with

adequate administrative, technical, and physical safeguards that meet defined requirement and standards to secure and protect sensitive customer information. Penalties include the possibility of FDIC insurance termination and fines for violations up to and above $1 million.

Federal Trade Commission Act §5 (FTC) 15 US Code § 45 or FTC Act Section 5 of 1914 is a federal law that regulates information security and mandates adequate cybersecurity strategies and policies from US organizations that are connected to the cloud except banks and common carriers. Penalties for this FTC Act §5 violation involve civil liabilities that have, in a recent Facebook case, reached $5 billion. This legislation is shrouded in ambiguity because it mandates organizations to engage in all reasonable and necessary security practices but fails to define these reasonable and necessary security practices.

The Health Insurance Portability and Accountability Act (HIPAA) 45 CFR Part 160, 45 CFR Part 164 was enacted to enforce information security privacy and breach reporting rules. HIPAA is mandatory to all entities that provide health care, manage health plans, clearinghouses and covered entities defined as business associates. HIPAA violators face fines that take into consideration the defaulting institutions concerted efforts in adhering to mandated responsibilities, the nature and extent of the violation and the degree to which an entity has endeavored to protect information. HIPAA violation fines have reached an all-time high of over $16 million.

Defense Federal Acquisition Regulation (DFAR) 48 CFR 252.204-7012 is a federal security and privacy law that regulates information security applicable to the US

Department of Defense (DoD) contractors. This regulation is mandates DoD contractors who process, store, or transmit defense information to implement and comply with adequate DoD security baselines and safeguards. Noncompliance may result in debarment.

Children's Online Privacy Protection Act (COPPA) is under title 15 of US Code Chapter 91, 16 CFR Part 312. COPPA is a federal privacy and cybersecurity law that regulates websites and online services content providers targeting children under 13. This law extends its provisions to include online content providers who are aware that their content or site is used by children under 13. The law regulates how under 13 online content providers collect, use, and disclose personal information from and about children. The FTC polices this Act with penalties that may result in fines that rise above $5.7 million and rising.

Regulations for the Use of Electronic Records in Clinical Investigations (FDA) is a Title 21 CFR Part 11 cybersecurity law under the Food and Drug Administration (FDA). This federal statute regulates how electronic records are accessed and used in clinical investigations by clinical investigators of medical products. Most of these entities are healthcare providers and are also compliant under HIPAA rules. The difference is that this law explicitly concerns IT systems and IT professionals. The federal government authorizes the FDA to enforce compliance and is empowered to conduct investigations and audits. This law ensures IT systems' accuracy, reliability, and consistent performance and to implement role-based access controls for individuals with the least privilege rights,

audit trails, develop and enforce written policies that ensure that individuals are accountable, and implement training awareness programs.

Commodity Futures Trading Commission Derivatives Clearing Organizations Regulation (CFTC) is a Title 17 CFR Part 39, Subpart B, 17 CFR 39.18 law that applies to global financial system derivative clearing entities. This law can attract civil fines for violations for up to one million dollars or three times the monetary gain. The law mandates derivative clearing entities to design and implement a robust program to manage their information security systems by providing annual compliance reports, use independent contractors to test for vulnerabilities twice quarterly, conduct annual internal and external penetration testing and tri-annual control testing, conduct annual security incident response plan testing and annual enterprise technology risk assessment (ETRA).

Electronic Communications Privacy Act and Stored Communications Act (ECPA & SCA) under title 18 of US Code Chapter 119 and 18 US Code Chapter 121 was initially designed to limit warrantless surveillance called the Wiretap Act. This federal privacy statute prohibits organizations from recording or disclosing any oral or electronic communications without prior consent. It requires that employers must have a valid business reason to electronically surveillance employees including video and email interception.

EU-US Privacy Shield is a joint US-EU law that seeks to protect the data of EU residents stored and processed by organizations in the US. The Privacy Shield was invalidated by the European Court of Justice (ECJ) soon as after its creation in 2020. Considering that large amounts of data are interchanged between the US and the EU,

commissioners of both governments created an alternative that met the EU's General Data Protection Regulation (GDPR) legal framework.

The Privacy Act of 1974 (FPA) applies only to US Federal Government agencies and is intended to govern the collection, maintenance, use, and dissemination of individuals' electronically stored PII by federal agencies. The FPA, which is empowered to fine defaulters up to $1,000.00 plus court charges and attorney fees protects the unlawful disclosure of information by a federal government agency without the subject's written consent. The law, however, has 12 statutory exceptions.

The Consumer Privacy Protection Act of 2017 was proposed in 2017 and is still being debated in Congress. If enacted into law, this Act shall target organizations that process sensitive information or PII of 10,000 or more US citizens in a calendar year. Penalties are expected to include civil fines of not more than $5 million with an additional 5 million dollars if the violation is proven to be willful or intentional.

A 2023 cloud security statistics report (Foundry, 2023) reported that 91% of US business institutions have some IT environment hosted in the cloud. The report concludes that despite the numerous benefits of cloud computing, companies need help scaling up to improve their cloud security posture to conform to data security and privacy challenges. The National Institute of Standards and Technology (NIST) has over the years and continuous to develop and made available to public and private entities alike cybersecurity best practices through frameworks and standards to help design, build, configure and manage cloud security.

The National Institute of Standards and Technology (NIST) is a US Department of Commerce agency with historically advanced innovative technology initiatives using its physical labs, guidelines, and standards. These standards include NIST cloud security best practices, requirements and frameworks that are designed to set a uniform code that cloud security professionals can tap from to build and maintain secure cloud environments.

In particular, NIST SP 800 – 53 and NIST SP 800 – 174 are special publications that content frameworks that address cloud computing and security controls and defines cloud security standards, policies, and best practices for cloud security professionals to manage cloud cyber security risks more efficiently (NIST, 2020).

The NIST Cybersecurity Framework provides solutions that enable IT professionals to mitigate cybersecurity vulnerabilities and reduce risks for all public and private sectors. It provides customizable specific security controls through its special publications which an entity can tailor to its unique environment. NIST 800 –53 is essential because it provides security controls for implementing NIST CSF. These security controls, particularly NIST SP 800 –53 and NIST SP 800 –145, aim to ensure that optimal security measures are applied to protect all cloud assets, including but not limited to risk assessments, data encryption, and installation of firewalls.

NIST cloud security standards Special Publications (SP) content technical requirements to help improve specifically cloud security. These Special Publications include:

1. SP 800 –144: These are guidelines on security and privacy in public cloud computing that address challenges facing public cloud security and privacy and provide recommendations as best practices. SP 800 –144 provides executives, IT and system managers who are policy makers in the information management realm with decision-making guidelines on how to carefully plan cloud computing solutions' security and privacy components before implementation. It also contents knowledge and understanding guidelines to enable providers to comply with organizational security and privacy accountability and compliance requirements to protect applications and data in the public cloud.
2. SP 800–145: Definition of Cloud Computing defines cloud computing, its characteristics and service models. Service models are composed of Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). Deployment models include private, community, public, and hybrid models. SP 800 –145offers a comparative view of cloud services within the cloud.
3. SP 800 –146: Cloud Computing Synopsis and Recommendations explains cloud systems and makes suggestions that can enable IT professionals to more coherently design different deployment and technical characteristics to manage such security concerns as cloud performance and reliability.
4. SP 800 –53: Security and Privacy Controls for Federal Information Systems and Organizations are specific security controls for federal agencies. SP 800 –

53standards define federal agencies' requirements and compliance standards with impact levels ranging from low, moderate, and high impact.

According to NIST, these are the relevant cloud security controls for organizations:

- access control
- audit and accountability
- configuration management
- identification and authentication
- risk assessment
- incident response

1. NIST SP 800 – 210: General Access Control Guidance for Cloud Systems addresses appropriate cloud access control measures for Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) service models.
2. NIST SP 800 – 500: provides security controls for implementing cloud security requirements based on NIST cybersecurity standards and controls that include risk assessments, access control, and configuration management.

NIST Cyber Security Framework

The NIST Cyber Security Framework was designed to help organizations of varied sectors and sizes reduce cybersecurity risks. NIST provides specific security controls through its special publications to facilitate easy customization of cybersecurity practices based on the unique mission of the individual company and its requirements.

NIST Cloud Security Best Practices

1. Continuous and consistent vulnerability assessments and penetration tests which are critically recommended by NIST because they aid in real-time detection, identification, exploitation, and mitigation of cloud vulnerabilities.
2. Install firewall and anti-malware software. NIST posits that robust firewalls are critical for scanning internal and external networks and proactively detecting viruses and worms in real time and filtering out signature based and zero-day suspicious traffic.
3. Encrypt data at rest and in transit to protect sensitive information from cybercriminals.
4. Implement identity and access management controls. Identity and access management provide and maintain access controls to secure cloud resources using multi-factor authentication (MFA), and role-based measures.
5. Incident response planning. NIST recommends institutions have incident response plans in place that define steps to mitigate, contain, and recover from security incidents (NIST, 2020).

Atkins & Lawson (2020) in a survey found that industry professionals and stakeholders contribute to and participate immensely in government exercises on the NIST cybersecurity framework.

NIST Benefits

- resilient and robust cloud security solutions

- tools and best practices that enable organizations to identify and mitigate risks in cloud environments.
- help organizations to comply with various cloud regulatory requirements such as SOC2, ISO 27001, and PCI-DSS
- recommends continuous monitoring to facilitate real-time threat detection and response.
- provides tools and frameworks that are very adaptable for public, private, community, or hybrid cloud deployment.
- improve efficiency and cost-effectiveness of resource usage

NIST cloud security standards, frameworks, and resources are invaluable in a world where cyber threats are rising exponentially. Implementing and maintaining NIST best practices and standards are critical to safeguard, secure and protect an organization's cloud security posture and save its reputation. Dudek et al (2020) in a survey of 125 certified German companies to analyze the adoption of ISO/IEC 27001, found implementation to be surprisingly low and concluded that its relevance may rise as stakeholders increasingly emphasis that companies take more active measures to safeguard information security.

Applications to Professional Practice

This study’s recommendations are intended to improve and change cloud cybersecurity practices. Fugue (2022) after analyzing survey data concluded that 36% of 300 cloud engineers and cybersecurity experts surveyed admitted having had a severe cloud security leak the previous year. There is exponential growth in data breaches of

cloud stored information at individual and organizational levels. The crucial essence of big data to the society has motivated hackers to attack information systems to install ransomware through which they infiltrate, compromise, and steal data thereby exacting enormous emotional, material, and reputational losses to individuals and the society. To prevent, mitigate and forestall trust, entities must invest in cybersecurity systems to preempt and protect critical national infrastructure. Jeyaraj & Zadeh (2022) studied internal cybersecurity strategies of some major US companies and found that organizations respond to cybersecurity threats by utilizing a mixture of exploration and exploitation measures to transition between quadrants since every organization uniquely encounters different cyber-threat types and also develops different strategies to respond and contend cyber-threats. The authors stated that General Dynamics encountered varied cybersecurity attempts to access its proprietary and classified information including threats to physical security of its facilities and employees using denial-of-service attacks. General Motors on the other hand developed its own access control measures to secure access to its IT infrastructure while Visa Corporation invested substantially to secure, protect, detect and respond to data security incidents. PepsiCo invested in security measures to secure its network by implementing backup and disaster recovery measures and capacity building competencies training programs for its employees.

The relevance and impact of the findings of this study on cloud information management may benefit professional cloud security practices because it informs the practice and adds new knowledge to the profession that is needed to improve and secure information. Chiara (2022) conducted a legal analysis of European Union cybersecurity

related legislation to investigate the extent to which existing and proposed legislation address the multitude of challenges posed by IoT and related services and concluded that the complexity of IoT technologies hinders the building of safeguards to ensure adequate levels of security and safety considering that each sector is unique with its own risk profile which also differ across sectors. The participants and publicly available information reviewed for this research provided experiential practices, strategies, and best practices that cloud security providers can implement to secure cloud infrastructure that is critical to national security. The need to secure cloud platforms is hampered by the lack of or limited knowledge of IT professionals, customers and the limitations of public awareness and attention. Nord et al (2022) reviewed literature on internet service providers in the US to investigate predictors of compliance and found that employees from new hires to CEOs from different sectors viewed supportive organizational culture and role values as significant predictor variables whereas leadership and engagement were less significant.

Findings from this study may enable and nudge cloud providers to perform regular risk assessments of their cloud infrastructure, employ IT professionals' expert knowledge to understand the implications of the actions implemented and to invest based on informed decision making so as to be proactive, preempt and stop an eminent attack rather than be reactive and respond to damage control. Though all IT professionals interviewed expressed the need and essence of protecting the cloud platforms, there was great variation in the strategies employed, number of annual investments and choice of technology purchased. It was however clear from their responses that each professional's

choice of initial security method has evolved over time due to the changing nature of threat actor's attack tactics and the rapid and unpredictable nature of technological advancement. The participants interviewed pointed at the fact that the choice of best practice and type of technology deployed was not always based on knowledge and skills but was often shaped by costs and what was available. This is not a good practice for corporations that understand the critical need to protect data. It is my fervent expectation that IT professionals and cloud provider decision makers will use these results as a foundation to re-access and improve their current practices and security methods and update their current processes and policies. These changes can be directed and tailored towards processes that address automation that minimizes human error by implementing rule-based processes to create user accounts and manage identity and access processes (Walton et al., 2021).

Corporate information management policies should ensure consistency and persistent application that conform and comply with frameworks and legal strictures throughout the corporation. Da Veiga (2016) conducted a comparative study of an experimental group who read corporate policy before implementing a task and a control group that did not and found that the experimental group participants had a positive perception of security policy and where readily in compliance with guidelines while the control group did not. For a cloud provider to affect change there must be a change management process in place that ensures effective communication within and without and the roles and responsibilities must be well defined and enforced. Successful change

can only occur if implementation has executive blessing and is properly planned and coordinated for any corporation to benefit from the findings of this study.

With technological advancement, the convenience of cloud-based computing availability with always-on connectivity has drastically changed the manner in which traditional IT security has been implemented and practiced. However, this functionality creates new loopholes and vulnerabilities that can be exploited by threat actors and thus demands new measures to secure the cloud platform. Jardine (2020) stated that new technology releases sometimes have ill effects on security outcomes in the short run and little-to-no effect over the long run and concluded from research results that the negative short-run effects on cybersecurity outcomes increasingly diminish at a predicted annual use rate of 7.03% after five years. Technological advancement has also enabled the creation and growth of digital tools where new releases of software and hardware, and the emergence of internet of things that has digitized homes and social services has effectively forced social change in the manner in which the society manages sedentary lifestyles. This has led to an increased need for cybersecurity solutions in which the detection of known or existing vulnerabilities and zero-day attacks becomes a challenge for cybersecurity professionals (Peppes et al., 2023). A major parentage of global businesses is small and medium-sized entities who are ill equipped to conduct research on their own but need research-based knowledge and solutions to understand the costs and reputational impact of possible cyber-attacks on their businesses and assets (Alharbi et al., 2021). Cyber-attacks and security events have enormous consequences for businesses and related stakeholders, which cause increases in investments in information

security. IT security investments decision making is usually based on a careful evaluation of risk factors, the effectiveness of existing solutions and evidence-based practices (Li et al., 2021). The literature points to the need for a balance between security and ease of use using best practices to design and provide solutions that feature both security and usability, but existing solutions tend to focus on either security or usability and not both (Faily & Flechais, 2011).

Some technology advancements have changed and benefited the society including the healthcare sector where the emergence and use of the Electronic Health Records (EHR) has proven to reduce healthcare costs, improve the quality care and the real-time delivery of healthcare services (Bhuyan et al., 2020). The EHR enables the use of sensor data and push notifications to detect fall incidents and provide real-time virtual care (Chen, 2022). The introduction of the EHR has led to increased interconnectivity and interoperability of medical devices information using the cloud platform but has also introduced security risks that pose a threat to the healthcare industry (Jones et al., 2022).

1. Data storage: Traditional IT models are designed based on costly and inflexible onsite data storage in contrast to cloud-based solutions that are more cost-effective in system development, reduced user control and maintenance.
2. Scaling speed: Cloud-based solutions are modular and can easily be commissioned, adapted to the unique organizational mission but pose security problems.
3. End-user interfacing: Cloud platforms are interconnected with networks and services that must be secured because of risks that range from unsecured end-

user devices, software and network level vulnerabilities to setup misconfigurations and user behaviors.

4. Proximity to other networked data and systems: Cloud platforms are connectivity based between cloud providers and users; thus, any defective device or wrong setup can be exploited, and privilege escalated to the entire system.

Implications for Social Change

Cybersecurity risks lead to consumer trust concerns. A Consumer Reports (2022) survey of 2,103 US adults reported that the last three years has seen significant positive changes to user cybersecurity and practices and that within one-year consumer online spending rose by 44%. A breach will severely expose user's information, punish brands, and cause social mistrust. When people cannot afford fuel to automate their vehicles or learn that their bank accounts had been breached and their personal data found on the dark web, they experience firsthand the impact cyber-attacks can have on their personal lives (Vijayan, 2023).

Data breaches come with psychological effects such as the WannaCry ransomware attack that led to disruption of critical infrastructure worldwide and severely impacted the U.K.'s National Health Service particularly scheduled procedures. WannaCry's impact included disruption of critical systems, affected individuals, and created real-time awareness risks for many (Akbanov & Vassilakis, 2019). It demonstrated how basic vulnerabilities in basic infrastructure could bring social change.

Cyber breaches cause service disruptions and depending on the nature of the breach, may be spread across a network or limited to a local infrastructure and are frustrating to individuals directly affected. A 2019 ransomware attack on a software vendor affected 22 Texas towns. The cybercriminals demanded $2.5 million to restore administrative services, and effectively prevented residents from accessing their records or pay utility bills (Bleiberg & Tucker, 2021). This study is intended to identify best practices that may help mitigate these increasing numbers of breaches.

Recommendations for Action

This study set out to investigate strategies that cloud security professionals implement to secure access and to protect data on their cloud infrastructure. To answer this question data was obtained from a telephone interview of cloud IT professionals and a thorough review of publicly available information including national and international standards and frameworks and laws government cybersecurity in general and cloud security in particular. The data collected using these two methods was thematically analyzed to answer the research question of how information stored in the cloud is secured and protected. From these information sources and a review of recent professional peer-reviewed literature on strategies to secure cloud infrastructure, I proffered some recommendations which security providers can implement to improve, update or reconfigure their cloud platforms.

1. Corporations should develop, implement, and enforce credible and effective security policies that meet the requirements of established frameworks and also compliant with existing laws and regulations.

2. Employees at all levels should be educated and trained to understand and comply with corporate policies and cybersecurity risk awareness. These training programs should be regular, employees tested, and the programs evaluated annually to measure and confirm effectiveness and adjustments made as necessary.
3. Corporations should ensure and implement continuous monitoring, risk assessments, incident response plans, proper events documentation, and mitigation plans.
4. Implement identity and access management methods that meet authorization and authentication industry specific standards which are tested regularly for effectiveness and updated to be resilient against both signature and zero-day attacks. There should be continuous and regularly scheduled impact assessments particularly when there is an instance of data transiting through the cloud (Cayirci et al, 2016). Though these measures require considerable investments in technology and personnel, it is a sine qua non for any corporation. Corporate buy
5. in is the necessary first step to any such investment either through third party company audits or internal IT departmental assessments, evaluation and resolving weak authentication methods.
6. Considering that there is reasonable user expectation for a fast and ease of use access to relevant information, there is a need for strategies that provide availability, confidentiality, and integrity and at the same time provide a

secure and robust system that guarantee operational efficiency (Shiferaw &Cerna, 2016). There is an urgent need for improved access and authentication strategies to include such trusted methods as multifactor authentication in identity and access management for remote access and onsite.

Recommendations for Further Study

The findings from this study are not conclusive and cannot be generalized to cover all aspects of cloud security since the focus of this study was identity and access control. Considering that cloud security is an emerging field and that new technology including software is released daily, there is literary warrant for further research in the field of cloud security infrastructure. Since the focus of this qualitative multiple-case study was on the experiences of cloud IT professionals and publicly available information, there is the need to examine corporate culture and organizational climate as possible major influences to the outcome of cloud security initiatives. The role that executives play in investment and policy making is of critical significance in protecting the cloud infrastructure and can determine the quality and quantity of IT professionals to hire and also determine what technology to purchase. Corporate buy in is essential in securing the cloud platform and demands further research. There is research needed to understand cloud user behaviors. According to research, human error contributes immensely to security breaches and needs further investigation. It is recommended that further research may be expanded to global audiences since many threat actors are hidden in rogue nations around the globe. Additional research is warranted to use the quantitative

methodology to test the role of investments as a ratio of security breaches when not addressed vis-a-vis the cost of implementing a secure system, the effect of user behaviors on the frequency and distribution of security vulnerabilities caused by users who received cybersecurity awareness training compared who did not receive the training.

Summary and Study Conclusions

Cloud computing has proven to be more advantageous over on-premises data centers due to its ability for data backup and ease of service restoration, redundancy, greater collaboration, accessibility, and affordability. However, cloud security challenges remain a major impediment to its adaptation and use. Issues that have led to known data breaches, unauthorized access, service disruptions, and potential loss of sensitive information undermine the trust and reliability that organizations and individuals place in cloud technologies. A good number of businesses are not knowledgeable and fail to understand their roles and responsibilities vis-a-vis that of cloud service providers (CSPs). This apparent ambiguity in role definition and the resultant failure by businesses to implement cloud security best practices is detrimental and endangers both national security interests, incurs corporate cost in material and reputational damages and torpedoes the lives of citizens especially when their private and sensitive information is sold on the dark web. According to the Cybersecurity Insiders (2023) 2023 Cloud Security Challenges Report, security is still a top concern for cloud users despite cloud computing's fast uptake. 76% of the cybersecurity experts surveyed in this research said they are very concerned about public cloud security. This study has attempted to provide solutions that may help further knowledge and understanding of the complicated area of

cloud security challenges. With the ever-evolving techniques of threat actors as well as the critical business investments in policy and technology, this study concludes that there is urgent need for action to ensure that cloud systems are secure and reliable and also need further research to broaden the knowledge base and inculcate an understanding of cloud cybersecurity as an emerging discipline. An entity's ability to secure a cloud network and protect data has proven to be very challenging. New untested technologies are released daily with unknown vulnerabilities and as cybercriminals keep inventing new tactics and always a step ahead of mitigation measures, IT professionals struggle to catch up. I have in this study endeavored to provide strategies and possible solutions to the aforementioned challenges to data being secured in the cloud. My aim has been to narrow the knowledge gap relating to cloud security. Society's fears and mistrust about the reliability of online systems and cloud computing are well founded considering the exponential and escalating number of data breaches that have in many cases found their personal and private information sold being sold on the dark web.

Though challenging and at times very complex, it takes a combination of risk assessments, experience, knowledge, resources, and enforced policies to secure and protect a network as there is no one-size fits all approach. The federal government's zero trust policy may be the panacea to information security management. Each entity is unique, and decisions are predicated on the critical business mission but the core lesson from this study is that they must implement strategies that are effective, compliment the business need with the overall goal being to secure and protect both human and material internal and external resources to guarantee user and stakeholder trust.

References

Abbas, H. S., Qaisar, Z. H., Ali, G., Alturise, F. & Alkhalifah, T. (2022). *Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare.* Plos One, 17(11*), e0274550* https://doi.org/10.1371/journal.pone.0274550

Ajzen, I. (2011). The theory of planned behavior: Reactions and reflections. *Psychology & Health*, *26*(9), 1113-127. https://doi.10.1080/08870446.2011.613995.

Alazab, M., Priya R. M., Parimala, M., Maddikunta, P. K. R., Gadekallu, T. R & Pham, Q. (2022). Federated learning for cybersecurity: Concepts, challenges, and future directions. *IEEE Transactions on Industrial Informatics*, *18*(5). https://ieeexplore.ieee.org/abstract/document/9566732

Alazzawi, F. R. Y., & Al-Wasiti. (2021). Requirements of formulating a national strategy for developing the cybersecurity system in Iraq according to GCI.v4(2019) Index. *Review of International Geographical Education (RIGEO)*, *11*(4), 49–71. https://doi.org/10.33403/rigeo.800625

Aldea, C. L., Bocu, R. & Vasilescu, A. (2022). Relevant cybersecurity aspects of IoT micro-services architectures deployed over next-generation mobile networks. *Sensors 2023, 23*, 189. https://doi.org/10.3390/s23010189

Alharbi, F., Alsulami, M., AL-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. *Sensors 2021, 21*,

6901. https://doi.org/10.3390/s21206901

Alomari, M. K., Khan, H. U., Khan, S., Al-Maadid, A. A., Zaki Khalid Abu-Shawish, Z. K., & Hammami, H. (2021). Systematic analysis of artificial intelligence-based platforms for identifying governance and access control. *Hindawi, Security and Communication Networks, 2021*. https://doi.org/10.1155/2021/8686469

Alqahtani, M. A. (2022). Cybersecurity awareness based on software and E-mail security with statistical analysis. *Hindawi, Computational Intelligence and Neuroscience, 2022*. https://doi.org/10.1155/2022/6775980

Alshabib, H. N., & Martins, J. T. (2022). Cybersecurity: Perceived threats and policy responses in the Gulf Cooperation Council. *IEEE Transactions on Engineering Management, 69*(6). https://doi.org/10.1109/TEM.2021.3083330

Arroyabe, I. F., Carlos F.A. Arranz, C. F. A., Arroyabe, M. F., Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security, 124*. https://doi.org/10.1016/j.cose.2022.102954

Ayaz, A., & Yanartaş, M. (2020). An analysis on the unified theory of acceptance and use of technology theory (UTAUT): Acceptance of electronic document management system (EDMS). *Computers in Human Behavior Reports, 2*, 100032. https://doi.org/10.1016/j.chbr.2020.100032

Aziz, A., Rasdi, R. M., Rami, A. A. & Razali, F. (2022). Factors determining academics' behavioral intention and usage behavior towards online teaching technologies during Covid-19: An extension of the UTAUT. *iJET, 17*(09).

https://doi.org/10.3991/ijet.v17i09.30481

Baldini, G. (2022). Detection of cybersecurity spoofing attacks in vehicular networks with recurrence quantification analysis. *Computer Communications*, *191*, 486–499. https://doi.org/10.1016/j.comcom.2022.05.021

Bans-Akutey, A., & Tiimub, B. (2021). Triangulation in research. Academia Letters, Article 3392. https://doi.org/10.20935/AL3

Baptista, G., & Oliveira, T. (2015). Understanding mobile banking: The unified theory of acceptance and use of technology combined with cultural moderators. *Computers in Human Behavior*, *50*. https://doi.org/10.1016/j.chb.2015.04.024

Barik, K., Misra, S., Konar, K., Fernandez-Sanz, L. & Koyuncu, M. (2022). Cybersecurity deep: Approaches, attacks dataset, and comparative study. *Applied Artificial Intelligence*, *36*(1), Article e2055399. https://doi.org/10.1080/08839514.2022.2055399

Barrett, David & Twycross, Alison. (2018). Data collection in qualitative research. Evidence Based Nursing. 21. ebnurs-2018. DOI:10.1136/eb-2018-102939.

Stefan Bauer, S., Bernroider, E. W. N. & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145–159. https://doi.org/10.1016/j.cose.2017.04.009

Bayaga, A., & du Plessis, A. (2023). Ramifications of the unified theory of acceptance and use of technology (UTAUT) among developing countries' higher education staffs. *Education and Information Technologies.* https://doi.org/10.1007/s10639-

023-12194-6

Bederna, Z., Rajnai, Z. & Szádeczky, T. (2021). (2021). Business strategy analysis of cybersecurity incidents. *Technical Sciences*. https://doi.org/10.2478/raft-2021-0020

Bederna, Z., Rajnai, Z. & Szádeczky, T. (2021b). Further strategy analysis of cybersecurity incidents. *Technical Sciences*. https://doi.org/10.2478/raft-2021-0032

Bhatti, B. M., Mubarak, S., & Nagalingam, S. (2021). Information Security Risk Management in IT Outsourcing – A Quarter-century Systematic Literature Review. Journal of Global Information Technology Management, 24(4), 259–298. https://doi.org/10.1080/1097198X.2021.1993725

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D. & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations. Journal of Medical Systems (2020) 44:98. https://doi.org/10.1007/s10916-019-1507-y

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

Bolbot, V. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of*

Critical Infrastructure Protection 39 (2022) 100571 https://doi.org/10.1016/j.ijcip.2022.100571

Bouzidi, M., Amro, A., Dalveren, Y., Cheikh, F. A., & Derawi, M. (2023). LPWAN cyber security risk analysis: Building a secure IQRF solution. *Sensors 2023, 23, 2078*. https://doi.org/10.3390/s23042078

Brailas, A., Tragou, E. & Papachristopoulos, K. (2023). Introduction to qualitative data analysis and coding with QualCoder. *American Journal of Qualitative Research. Vol. 7 No. 3, pp. 19-31*. https://doi.org/10.29333/ajqr/13230

Bramo, S. S., Desta, A. & Syedda, M. (2022). Acceptance of information communication technology-based health information services: Exploring the culture in primary-level health care of South Ethiopia, using UTAUT Model, Ethnographic Study. *Digital Health*. doi:10.1177/20552076221131144

Brett, D. & Woelfel, T. (2019). Impact due diligence: Emerging best practices, a synthesis of due diligence practices employed by leading impact investors who systematically assess investments' anticipated impact. The Pacific Community Ventures. https://www.pacificcommunityventures.org/wp-content/uploads/sites/6/Impact-Due-Diligence-Emerging-Best-Practices_website.pdf

Brown, S. A., & Venkatesh, V. (2005). Model of adoption of technology in households: A Baseline Model Test and Extension Incorporating Household Life Cycle. *MIS Quarterly, 29(3), 399–426.* https://doi.org/10.2307/25148690

Bruggemann, R. et al. (2021). Global Cybersecurity Index (GCI) and the role of its 5

pillars. *Social Indicators Research (2022) 159:125–143.* https://doi.org/10.1007/s11205-021-02739-y

Bruzgiene, R. & Jurgilas, K. (2021). Securing remote access to information systems of critical infrastructure using two-factor authentication. *Electronics 2021, 10, 1819.* https://doi.org/10.3390/ electronics10151819

Cai, C. & Zhao, L. (2023). Information sharing and deferral option in cybersecurity investment. *Plos One18(2): e0281314.* https://doi.org/10.1371/journal.pone.0281314

Calcara, A. & Marchetti, R. (2022). State-industry relations and cybersecurity governance in Europe. *Review of International Political Economy, 29:4, 1237-1262.* doi:10.1080/09692290.2021.1913438

Candela, A. G. (2019). Exploring the function of member checking. *The Qualitative Report, 24(3), 619–628.* https://doi.org/10.46743/2160-3715/2019.3726

Carayannis, E. C. et al. (2021). Ambidextrous cybersecurity: The seven pillars (7Ps) of cyber resilience. *IEEE Transactions on Engineering Management, Vol. 68, No. 1, February 2021.* https://www.ieee.org/publications/rights/index.html

Chapman, T. A. & Reithel, B. J. (2021). Perceptions of cybersecurity readiness among workgroup IT managers. *Journal of Computer Information Systems, 61:5, 438-449.* doi:10.1080/08874417.2019.1703224

Casteel, Alex & Bridier, Nancy. (2021). Describing populations and samples in doctoral student research. *International Journal of Doctoral Studies*. 16. 339-362. https://doi.10.28945/4766.

Chatti, H. & Hadoussa, S. (2021). Factors affecting the adoption of e-learning technology by students during the covid-19 quarantine period: The application of the UTAUT model. *Engineering, Technology & Applied Science Research Vol. 11, No. 2, 2021, 6993-7000.* doi:10.48084/etasr.3985

Chauvette, A., Schick-Makaroff, K., & Molzahn, A. E. (2019). Open data in qualitative research. *International Journal of Qualitative Methods, 18.* https://doi.org/10.1177/1609406918823863

Chang, Andreas. (2012). UTAUT and UTAUT 2: A Review and Agenda for Future Research. *The Winners. 13. 10.* https://doi:10.21512/tw.v13i2.656

Chauhan, S., Jaiswal, M & Kar, A. K. (2018). The Acceptance of Electronic Voting Machines in India: A UTAUT approach. *Electronic Government, an International Journal. 14. 1.* https://doi:10.1504/EG.2018.10011841

Chen, M. (2022). Establishing a cybersecurity home monitoring system for the elderly. *IEEE Transactions on Industrial Informatics, VOL. 18, NO. 7, JULY 2022.* https://10.1109/TII.2021.3114296

Chen, Y. et al. (2013). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems / Winter 2012–13, Vol. 29, No. 3, 157–188.* https://doi:10.2753/MIS0742-1222290305

Chen, Y. (2022). Information security management: Compliance challenges and new directions. *Journal of Information Technology Case and Application Research, 24:4, 243-249.* https://doi:10.1080/15228053.2022.2148979

Chiara, P. G. (2022) The IoT and the new EU cybersecurity regulatory landscape.

International Review of Law, Computers & Technology, 36:2, 118-137. https://doi:10.1080/13600869.2022.2060468

Chodakowska, A., Kańduła, S. & Przybylska, J. (2022). Cybersecurity in the local government sector in Poland: More work needs to be done. *Lex Localis- Journal of Local Self-Government Vol. 20, No. 1, pp. 161 – 192, January 2022.* https://doi.org/10.4335/20.1.161-192(2022)

CISA. (2018). Indicators associated with WannaCry ransomware. https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware. https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware

Clim, A. et al. (2022). The Need for cybersecurity in industrial revolution and smart cities. *Sensors 2023, 23, 120.* https://doi.org/ 10.3390/s23010120

Collins, C. S., & Stockton, C. (2022). The theater of qualitative research: The role of the researcher/actor. *International Journal of Qualitative Methods, 21.* https://doi.org/10.1177/16094069221103109

Cordente-Rodriguez, M., Simone Splendiani, S. & Silvestrelli, P. (2020). Measuring propensity of online purchase by using the tam model: Evidence from Italian university students. *Applied Computer Science, vol. 16, no. 2, pp. 32–52* doi:10.23743/acs-2020-11

Corman, A. A., Rodríguez, D. F, Georgiou, M. V., Rische, J., Schuszter, I. C., Short, H. & Tedesco, P.. (2020). CERN's identity and access management: *A journey to open source. EPJ Web of Conferences 245, 03012 (2020) CHEP 2019.*

https://doi.org/10.1051/epjconf/202024503012

Crabtree, B. F., & Miller, W. L. (2023). Doing qualitative research (3rd ed.). SAGE Publications. https://www.vitalsource.com/products/doing-qualitative-research-benjamin-f-crabtree-william-v9781506302829

Cram, W. A. et al. (2020). Maximizing employee compliance with cybersecurity policies. MIS Quarterly Executive, September 2020 (19:3). https://doi:10.17705/2msqe.00032

Davis, F. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies, Volume 38, Issue 3, 1993, Pages 475-487.* https://doi.org/10.1006/imms.1993.1022.

Dhirani, L., Mukhtiar, N., Chowdhry, B. S. & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. *Sensors 2023, 23, 1151.* https://doi.org/10.3390/s23031151

DomingoFerrer, J. & BlancoJusticia, A. (2019). Ethical value-centric cybersecurity: A methodology based on a value graph. *Science and Engineering Ethics (2020) 26:1267–1285.* https://doi.org/10.1007/s11948-019-00138-8

Dwivedi, Y., Rana, N., Jeyaraj, A., Clement, M. & Williams, M. (2019). Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a revised theoretical model. *Inf Syst Front 21, 719–734 (2019).* https://doi.org/10.1007/s10796-017-9774-y

Dwivedi, Y., Rana, N., Tamilmani, K. & Raman, R. (2020). A meta-analysis based

modified unified theory of acceptance and use of technology (meta-UTAUT): A review of emerging literature. *Volume 36, 2020, pp 13-18.* https://doi.org/10.1016/j.copsyc.2020.03.008. https://www.sciencedirect.com/science/article/pii/S2352250X20300373

Dunwoodie, K., Macaulay, L. & Newman, A. (2022). Qualitative interviewing in the field of work and organizational psychology: Benefits, challenges and guidelines for researchers and reviewers. Applied Psychology. 72. https://doi.10.1111/apps.12414.

Dykstra, J. (2022). Action bias and the two most dangerous words in cybersecurity incident response: An argument for more measured incident response. *IEEE Security & Privacy, vol. 20, no. 3, pp. 102-106, May-June 2022.* https://doi: 10.1109/MSEC.2022.3159471

Eastwood, B. (2022). Cloud adoption linked to stronger firm performance. *MIT Sloan School of Management.* https://mitsloan.mit.edu/ideas-made-to-matter/cloud-adoption-linked-to-stronger-firm-performance.

Eichelberg, M., Kleber, K. & Kämmerer, M. (2020). Cybersecurity in PACS and medical imaging: An overview. *Journal of Digital Imaging (2020) 33:1527–1542 Vol.:(0123456789) 13.* https://doi.org/10.1007/s10278-020-00393-3

Elhami, A. & Khoshnevisan, B. (2022). Conducting an interview in qualitative research: The modus operandi. *MEXTESOL Journal, Vol. 46, No. 1, 2022.* https://files.eric.ed.gov/fulltext/EJ1333875.pdf

Ellis, P. (2021). Sampling in qualitative research (3). *Wounds UK, 17(1), 128–130.*

https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=14&sid=0e24bd5d-70c8-428b-a199-9645fb1c03c1%40redis

Emer, A. et al. (2021). A cybersecurity assessment model for small and medium-sized enterprises. *IEEE Engineering Management Review, VOL. 49, No. 2, Second Quarter, June 2021. IEEE.* https://doi:10.1109/EMR.2021.3078077.

Faily, S. & Flechais. (2011). User-centered information security policy development in a post-Stuxnet world. *IEEE, Computer Society*. https://doi:10.1109/ARES.2011.111

Farahbod, K., Shayo, C. & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. *Journal of Business and Behavioral Sciences Vol 32, No 1; Spring 2020.* https://www.proquest.com/scholarly-journals/cybersecurity-indices-cybercrime-annual-loss/docview/2426140034/se-2

Farrand, B. & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security, 31:3, 435-453.* https://doi:10.1080/09662839.2022.2102896

Georg-Schaffner, L. & Prinz, E. (2021). Corporate management boards' information security orientation: An analysis of cybersecurity incidents in DAX 30 companies. *Journal of Management and Governance (2022) 26:1375–1408* https://doi.org/10.1007/s10997-021-09588-4

Ghahramani, F., Yazdanmehr, A., Chen, D., & Wang, J. (2023). Continuous improvement of information security management: An organizational learning perspective. *European Journal of Information Systems, 32(6), 1011–1032.* https://doi.org/10.1080/0960085X.2022.2096491

Golightly L, Chang V, Xu Qa, Gao X, Liu B.S. (2022). Adoption of cloud computing as innovation in the organization. *International Journal of Engineering Business Management. 2022;14.* https://doi:10.1177/18479790221093992

González-Granadillo, G., González-Zarzosa, S. & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors 2021, 21, 4759.* https://doi.org/10.3390/s21144759

Gupta, A., Dasgupta, S. & Gupta, A. (2008) Adoption of ICT in a government organization in a developing country: An Empirical study. *The Journal of Strategic Information Systems, 17, 140-154.* https://doi.org/10.1016/j.jsis.2007.12.004

Gyure, M., Quillin, J., Rodríguez, V., Markowitz, M., Corona, R., Borzelleca, J., Bowen, D., Krist, A. & Bodurtha, J. (2014). Practical considerations for implementing research recruitment etiquette. *IRB. 2014 Nov-Dec;36(6):7-12. PMID: 25684834; PMCID: PMC4324645.* https://www.researchgate.net/publication/272358526_Practical_Considerations_for_Implementing_Research_Recruitment_Etiquette

Hayashi Jr, P., Abib, G. & Hoppen, N. (2019). Validity in qualitative research: A processual approach. *The Qualitative Report 2019 Volume 24, Number 1, How-To Article 3, 98-112.* https://nsuworks.nova.edu/tqr/vol24/iss1/8 https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=3443&context=tqr

He, C. Z. Frost, T. & Pinsker, R. E. (2020). The impact of reported cybersecurity breaches on firm innovation. *Journal of Information Systems. Vol. 34, No. 2.*

Summer 2020 pp. 187–209. https://doi.10.2308/isys-18-053

Hewavitharana, T., Nanayakkara, S., Perera, A. & Perera, P. (2021). Modifying the Unified Theory of Acceptance and Use of Technology (UTAUT) model for the digital transformation of the construction industry from the user perspective. *Informatics 2021, 8, 81*. https://doi.org/10.3390/informatics8040081

Huang, K., Madnick, S., Choucri, N. & Zhang, F. (2021). A systematic framework to understand transnational governance for cybersecurity risks from digital trade. *Global Policy Volume 12. Issue 5*. https://doi:10.1111/1758-5899.13014

Hurel, L. M. (2022) Interrogating the cybersecurity development agenda: A critical reflection. *The International Spectator, 57:3, 66-84.* https://doi:10.1080/03932729.2022.2095824

Hijji, M. & Alam, G. (2022). Cybersecurity awareness and training (CAT) framework for remote working employees. *Sensors 2022, 22, 8663*. https://doi.org/ 10.3390/s22228663

Ifinedo, P. (2023). Effects of security knowledge, self-control, and countermeasures on cybersecurity behaviors. *Journal of Computer Information Systems 2023, VOL. 63, NO. 2, 380–396*. https://doi.org/10.1080/08874417.2022.2065553

Im, I., Hong, S., & Kang, M. S. (2011). An international comparison of technology adoption testing the UTAUT model. *Information & Management. 48. 1-8.* https://doi:10.1016/j.im.2010.09.001.

Institutional Review Board. (2024). Research ethics review process by IRB. *Walden University Office of Research and Doctoral Services.*

https://academicguides.waldenu.edu/research-center/research-ethics/review-process

Jalili, V., Afgan, E., Taylor, J., & Goecks, J. (2019). Cloud bursting galaxy: Federated identity and access management. *Bioinformatics, 36(1), 2020, 1–9. DOI: 10.1093/bioinformatics/btz472* https://opensource.org/licenses/AFL-3.0

Jardine, E. (2020). The case against commercial antivirus software: Risk homeostasis and information problems in cybersecurity. *Risk Analysis, Vol. 40, No. 8, 2020. DOI: 10.1111/risa.13534* https://doi.10.1111/risa.13534

Jeyaraj, A. & Zadeh, A. H. (2022). Exploration and exploitation in organizational cybersecurity. *Journal of Computer Information Systems, 62:4, 680-693.* https://doi.10.1080/08874417.2021.1902424

Jeyaraj, A., Amir Zadeh, A. & Sethi, V. (2020). Cybersecurity threats and organizational response: Textual analysis and panel regression. *Journal of Business Analytics 2021, VOL. 4, NO. 1, 26–39.* https://doi.org/10.1080/2573234X.2020.1863750

Jilcha, K. (2019). Research design and methodology. Doi:10.5772/intechopen.85731.

Jin, W. & Bai, J. (2022). Cloud adoption and firm performance: Evidence from labor demand. *July 25, 2022*. https://ssrn.com/abstract=4082436 http://dx.doi.org/10.2139/ssrn.4082436

Jones, D., Greenhill, R., Shaw, C., Flores, D. & Schmidt, R. N. (2022). Cybersecurity threats in the healthcare industry. *Journal of Business and Educational Leadership Vol 12, No 1; Summer 2022.*

Johnson, J. L. et al. (2020). A Review of the quality indicators of rigor in qualitative

research. *Qualitative Research in Pharmacy Education. Volume 84, Issue 1, 7120, January 01, 2020.* https://doi.org/10.5688/ajpe7120

Kabanov, I. &Madnick, S. (2021). Applying the lessons from the Equifax cybersecurity incident to build a better defense. *MIS Quarterly Executive, June 2021 (20:2).* https://doi:10.17705/2msqe.00044

Kanciak, K. & Wrona, K. (2020). Towards an auditable cryptographic access control to high-value sensitive data. *Intl Journal of Electronics and Telecommunications, 2020, NO. 3, PP. 449-458.* https://doi.10.24425/ijet.2020.131898

Kang, M., Hovav, A., Lee, E.T., Um, S. & Kim, H. (2022). Development of methods for identifying an appropriate benchmarking peer to establish information security policy. *Expert Systems with Applications, Volume 201, 2022.* https://doi.org/10.1016/j.eswa.2022.117028. https://www.sciencedirect.com/science/article/pii/S0957417422004444

Kang, M. & Hovav, A. (2018). Benchmarking methodology for Information Security Policy (BMISP): Artifact development and evaluation. *Information Systems Frontiers, 22:221–242.* https://doi.org/10.1007/s10796-018-9855-6

Kapiszewski, D., & Karcher, S. (2021). Transparency in practice in qualitative research. *Political Science & Politics, 54(2), 285–291.* https://doi.org/10.1017/S1049096520000955

Karlsson, F., Kolkowska, E. & Petersson, J. (2021). Information security policy compliance-eliciting requirements for computerized software to support value-based compliance analysis. *Elsevier, Computers & Security 114 (2022) 102578.*

https://doi.org/10.1016/j.cose.2021.102578

Kelton, A. & Pennington, R.R. (2020). Do voluntary disclosures mitigate the cybersecurity breach contagion effect? *Journal of Information Systems American Accounting Association Vol. 34, No. 3*. https://doi.10.2308/isys-52628 Fall 2020 pp. 133–157

Khanday, S. & Khanam, D. (2023). The research design. *Journal of Critical Reviews, Vol 06, Issue 03, 2019.* https://www.researchgate.net/publication/368257495_The_Research_Design

Kianpour, M. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory, Volume 116, 2022, 102493.* https://doi.org/10.1016/j.simpat.2022.102493. https://www.sciencedirect.com/science/article/pii/S1569190X22000053

Kim, D. & Kim, S. (2021). Reframing South Korea's national cybersecurity governance system in critical information infrastructure. *The Korean Journal of Defense Analysis Vol. 33, No. 4, December 2021, 689 ─713* https://doi.org/10.22883/kjda.2021.33.4.007

Krutilla, K., Alexeev, A., Jardine, E. & Good, D. (2021). The benefits and costs of cybersecurity risk reduction: A dynamic extension of the Gordon and Loeb model. *Risk Analysis, Vol. 41, No. 10, 2021*. https://doi.10.1111/risa.13713

Leal, M. M. & Musgrave, P. (2022). Hitting back or holding back in cyberspace: Experimental evidence regarding Americans' responses to cyberattacks. *Conflict Management and Peace Science 2023, Vol. 40(1) 42–64.*

https://doi.10.1177/07388942221111069

Lewallen, J. (2021). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance (2021) 15, 1035–1052.* https://doi:10.1111/rego.12341

Li, H. et al. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. *Journal of Management Information Systems 2021, VOL. 38, NO. 1, 222–245* https://doi.org/10.1080/07421222.2021.1870390

Lin, B. et al. (2023). Information security protection of internet of energy using ensemble public key algorithm under big data. *Hindawi, Journal of Electrical and Computer Engineering Volume 2023.* https://doi.org/10.1155/2023/6853902

Lindheim, T. (2022). Participant validation: A strategy to strengthen the trustworthiness of your study and address ethical concerns. Espedal, G., JelstadLøvaas, B., Sirris, S., Wæraas, A. (eds) Researching Values. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-90769-3_13

Linneberg, M. &Korsgaard, S. (2019). Coding qualitative data: A synthesis guiding the novice. *Qualitative Research Journal.* https://doi.10.1108/QRJ-12-2018-0012.

Liu, Z. et al. (2021). Using event-based methods to estimate cybersecurity equilibrium. IEEE/CAA. *Journal of AutomaticaSinica, Vol. 8, No. 2, February 2021*. https://doi.10.1109/JAS.2020.1003527

Loishyn, A. et al. (2021). Development of the concept of cybersecurity of the organization. TEM Journal. Volume 10, Issue 3, 1447-1453. DOI: 10.18421/TEM103-57 https://doi.org/10.18421/TEM103-57

McKim, C. (2023). Meaningful Member-Checking: A structured approach to member checking. *American Journal of Qualitative Research 2023, Vol. 7 No. 2, pp. 41-52*. https://doi.org/10.29333/ajqr/12973

Maietta, J. T. (2020). Integrating illness management into identity verification processes. *Qualitative Health Research 2021, Vol. 31(2) 254–270*. https://doi.org/10.1177/1049732320966

Majid, M. A. A. et al. (2017). Piloting for interviews in qualitative research: Operationalization and lessons learnt. *International Journal of Academic Research in Business and Social Sciences. 2017, Vol. 7, No. 4.* https://hrmars.com/papers_submitted/2916/Piloting_for_Interviews_in_Qualitative_Research_Operationalization_and_Lessons_Learnt.pdf

Marikyan, D. & Papagiannidis, S. (2023) Unified Theory of Acceptance and Use of Technology: A review. *In S. Papagiannidis (Ed), TheoryHub Book.* https://open.ncl.ac.uk

Matar, N. et al. (2020). Factors affecting behavioral intentions towards cloud computing in the workplace: A case analysis for Jordanian universities. *iJET – Vol. 15, No. 16, 2020*. https://doi.org/10.3991/ijet.v15i16.14811

Matheu, S. N. et al. (2020). A survey of cybersecurity certification for the internet of things. *ACM Comput. Surv. 53, 6, Article 115*. https://doi.org/10.1145/3410160

Megheirkouni, M. & Moir, J. (2023). Simple but effective criteria: Rethinking excellent qualitative research. *The Qualitative Report, 28(3), 848-864.* https://doi.org/10.46743/2160-3715/2023.5845

Mendoza, A. L. et al. (2023). Cybersecurity among university students from Generation Z: A comparative study of the undergraduate Programs in Administration and Public Accounting in two Mexican universities. *TEM Journal. Volume 12, Issue 1, pages 503-511, ISSN 2217-8309.* https://doi.10.18421/TEM121-60.

Mirtsch, M. et al. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Elsevier, Computers & Security 109 (2021) 102383*. http://creativecommons.org/licenses/by/4.0/

Mirtsch, M. (2021). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A web mining-based analysis. *IEEE Transactions on Engineering Management, VOL. 68, NO. 1, February 2021*. https://doi.10.1109/TEM.2020.2977815

Mishra, A. et al. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors 2022, 22, 538*. https://doi.org/10.3390/s22020538

Mogashoa, T. (2014). Understanding critical discourse analysis in qualitative research. *International Journal of Humanities Social Sciences and Education (IJHSSE). Volume 1, Issue 7, July 2014, PP 104-113*. https://www.arcjournals.org/pdfs/ijhsse/v1-i7/12.pdf

Muhammad, Z. et al. (2023). Cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability. *Energies 2023, 16*. https://doi.org/10.3390/en16031113

Mütterlein, J. et al. (2019). Effects of lead-usership on the acceptance of media innovations: A mobile augmented reality case. *Technological Forecasting and*

Social Change. 145. 113-124. https://doi.10.1016/j.techfore.2019.04.019.

Mwita, Kelvin. (2022). Factors influencing data saturation in qualitative studies. *International Journal of Research in Business and Social Science (2147-4478).* 11. 414-420. https://doi.10.20525/ijrbs.v11i4.1776.

National Institute of Standards and Technology (NIST). (2020). Security and privacy controls for information systems and organizations: *NIST Special Publication 800-53 Revision 5. Joint Task Force.* https://doi.org/10.6028/NIST.SP.800-53r5

Negrin, K. A.et al. (2022). Successful recruitment to qualitative research: A critical reflection. *International Journal of Qualitative Methods, 21*. https://doi.org/10.1177/16094069221119576

Noble, N. &Heale, R. (2019). Triangulation in research, with examples. *BMJ Journals,22(3).* https://ebn.bmj.com/content/22/3/67

Nord, J. et al. (2022) Predictors of success in information security policy compliance. *Journal of Computer Information Systems, 62:4, 863-873*. https://doi.10.1080/08874417.2022.2067795

Nyirenda, L.et al. (2020). Using research networks to generate trustworthy qualitative public health research findings from multiple contexts. *BMC Med Res Methodol 20, 13 (2020)*. https://doi.org/10.1186/s12874-019-0895-5

Omam, L.A. et al. (2023). Refinement pathway for quality research interview guides: An 8-step process to refine a protocol for a complex multi-country humanitarian study. *Journal of Global Health Reports. 2023;7:e2023065*. https://doi.10.29392/001c.87858

OXFAM. (2020). Research ethics: A practical guide. https://oxfamilibrary.openrepository.com/bitstream/handle/10546/621092/gd-research-ethics-practical-guide-091120-en.pdf;jsessionid=0F17889B0F846F657CDD4B0AB3E3A749?sequence=1 https://doi.10.21201/2020.6416

Ozdemir, S. et al. (2022). Cybersecurity and country of origin: Towards a new framework for assessing digital product domesticity. *Sustainability 2023, 15, 87*. https://doi.org/ 10.3390/su15010087

Park, S. et al. (2022). Configuration method of AWS security architecture is applicable to the cloud lifecycle for sustainable social network. *Hindawi, Security and Communication Networks Volume 2022*. https://doi.org/10.1155/2022/3686423

Partida, A. et al. (2021). Identity and access management resilience against intentional risk for blockchain-based IOT platforms. *Electronics 2021, 10, 378*. https://doi.org/10.3390/ electronics10040378

Patel, D. (2020). Scope and usage of discourse analysis as a research method in English studies. *International Journal for Innovative Research in Multidisciplinary Field. Volume - 6, Issue - 3, Mar – 2020*. https://www.ijirmf.com/wp-content/uploads/IJIRMF202003042.pdf

Patton, M. Q. (2015). Qualitative evaluation and research methods. Thousand Oaks, CA: Sage. https://us.sagepub.com/en-us/nam/qualitative-research-evaluation-methods/book232962

Peppes, N. et al. (2023). The effectiveness of zero-day attacks data samples generated via

GANs on deep learning classifiers. *Sensors 2023, 23, 900*. https://doi.org/10.3390/s23020900

Pharmaceutical Inspection Convention. (2021). Good practices for data management and integrity in regulated GMP/GDP environments. https://picscheme.org/docview/423

Pinto, S.J. et al. (2023). Review of cybersecurity analysis in smart distribution systems and future directions for using unsupervised learning methods for cyber detection. *Energies 2023, 16, 1651*. https://doi.org/10.3390/ en16041651

Ponce, H. G. et al. (2021). Sustainable finance in cybersecurity investment for future profitability under uncertainty. *Journal of Sustainable Finance & Investment 2023, Vol. 13, NO. 1, 614–633* https://doi.org/10.1080/20430795.2021.1985951

Popova, Y. & Zagulova, D. (2022). UTAUT model for smart city concept implementation: Use of web applications by residents for everyday operations. *Informatics 2022, 9, 27*. https://doi.org/10.3390/ informatics9010027

Potthoff, S. (2023). Research ethics in qualitative health research. *International Journal of Qualitative Methods, 1–3*. https://doi.org/10.1177/16094069231189335

Ramezan, C. A. (2023). Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field. *Journal of Information System Education, 34(1), 94-105, Winter 2023*. https://www.researchgate.net/publication/370049722_Examining_the_Cyber_Skills_Gap_An_Analysis_of_Cybersecurity_Positions_by_Sub-Field

Rahman, Rafidah Binti Ab (2023). Comparison of telephone and in-person interviews for

data collection in qualitative human research. University of Illinois at Chicago. Journal contribution. https://doi.org/10.25417/uic.22217215.v1

Rawat, D. et al. (2021). Cybersecurity in big data era: From securing big data to data-driven security. *IEEE Transactions on Services Computing, Vol. 14, No. 6, November/December 2021*. https://doi.10.1109/TSC.2019.2907247

Rostami, E. et al. Requirements for computerized tools to design information security policies. *Elsevier, Computers & Security 99 (2020) 102063*. https://doi.org/10.1016/j.cose.2020.102063

Roy, J. (2020). Overview of customer identity and access management. *ISSA Journal*.

Russell, G. M., & Kelly, N. H. (2002, September). Research as interacting dialogic processes: Implications for reflexivity. *In Forum Qualitative Sozialforschung/Forum: Qualitative Social Research (Vol. 3, No. 3).*

Salat, L. et al. (2023). DNS tunneling, exfiltration and detection over cloud environments. *Sensors 2023, 23, 2760*. https://doi.org/10.3390/s23052760

Samuel, G. et al., 2019). The ethics ecosystem: Personal ethics, network governance and regulating actors governing the use of social media research data. *Minerva 57, 317– 343 (2019).* https://doi.org/10.1007/s11024-019-09368-3

Sawik, T. & Sawik, B. (2021). A rough-cut cybersecurity investment using portfolio of security controls with maximum cybersecurity value. *International Journal of Production Research 2022, Vol. 60, NO. 21, 6556–6572* https://doi.org/10.1080/00207543.2021.1994166

Sean Atkins, S. & Lawson, C. (2020). An improvised patchwork: Success and failure in

cybersecurity policy for critical infrastructure. *Public Administration Review, Vol. 81, ISS. 5, pp. 847–861. © 2020 by The American Society for Public Administration*. https://doi.10.1111/puar.13322.

Shaheen, M. et al. (2019). Sampling in qualitative research. 10.4018/978-1-5225-5366-3.ch002.

Shaikh, F. A. &Siponen, M. (2022). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Elsevier, Computers & Security 124 (2023)*. https://doi.org/10.1016/j.cose.2022.102974

Shakir, M. & Rahman, A. (2022). Conducting Pilot study in a qualitative inquiry: Learning some useful lessons. *Journal of Positive School Psychology, 2022, Vol. 6, No. 10, 1620-1624*. http://journalppw.com

Sheppard, B. et al (1988). The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research. *Journal of Consumer Research. 15*. https://doi.10.1086/209170.

Slapnicar, S. et al. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems 44 (2022) 100548.* https://doi.org/10.1016/j.accinf.2021.100548

Sobel, A. & Vetter, R. (2023). Cybersecurity best practices for CISE programs. *THE IEEE Computer Society*. https://doi.10.1109/MC.2021.3109841

Solms, R. V. et al. (2011). Information security governance control through comprehensive policy architectures. *IEEE*

Soni, P. et al. (2023). Cybersecurity attack-resilience authentication mechanism for intelligent healthcare system. *IEEE Transactions on Industrial Informatics, Vol. 19, No. 1*. https://www.ieee.org/publications/rights/index.html

Sousa, P.R. et al. (2021). Provisioning, authentication and secure communications for IoT devices on FIWARE. *Sensors 2021, 21, 5898*. https://10.3390/s2117589

Stahl, N. A. & King, J. R. (2020). Expanding approaches for research: Understanding and using trustworthiness in qualitative research. https://files.eric.ed.gov/fulltext/EJ1320570.pdf

Stoynov, S. &Nikolov, B. (2021). Approach to ship's IT and OT systems cybersecurity improvement. *Pedagogika-Pedagogy. Volume93, Number 7s, 2021*. https://doi.org/10.53656/ped21-7s.16appr

Subedi, M. (2023). Sampling and trustworthiness issues in qualitative research. *Dhaulagiri: Journal of Sociology & Anthropology, 17(1), 61–64.* https://doi.org/10.3126/dsaj.v17i01.61146

Subedi, Khim. (2021). Determining the Sample in Qualitative Research. *Scholars' Journal. 1-13. 10.3126/scholars.v4i1.42457*. https://doi.10.3126/scholars.v4i1.42457

Suciu, Lavinia. (2023). Qualitative research approaches and designs: Discourse analysis. https://www.researchgate.net/publication/369763176_Qualitative_research_approaches_and_designs_discourse_analysis

Szczepaniuk, E. K. & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. Telecommunications Policy,

Volume 46, Issue 3. https://doi.org/10.1016/j.telpol.2021.102282. https://www.sciencedirect.com/science/article/pii/S0308596121001865

Taherdoost, Hamed. (2022). Designing a questionnaire for a research paper: A comprehensive guide to design and develop an effective questionnaire. *Asian Journal of Managerial Science, Vol.11 No.1, 2022, pp.8-16*. https://doi.org/10.51983/ajms-2022.11.1.3087

Taiwo, A.& Downe, A. (2013). The theory of user acceptance and use of technology (UTAUT): A meta-analytic review of empirical findings. Journal of Theoretical and Applied Information Technology. 49. 48-58. https://www.researchgate.net/publication/279653519_The_theory_of_user_acceptance_and_use_of_technology_UTAUT_A_meta-analytic_review_of_empirical_findings.

Tanantong, T. & Wongras, P. (2024). A UTAUT-based framework for analyzing users' intention to adopt artificial intelligence in human resource recruitment: A case study of Thailand. *Systems 2024, 12, 28*. https://doi.org/10.3390/systems12010028

Tasheva, I. (2021). Cybersecurity post-COVID-19: Lessons learned and policy recommendations. *European View 2021, Vol. 20(2) 140–149*. https://doi.10.1177/17816858211059250

Tasheva, I. & Kunkel, I. (2022). In a hyper connected world, is the EU cybersecurity framework connected? *European View 2022, Vol. 21(2) 186–195*. https://doi.10.1177/17816858221136106

Tenny, S.et al. (2022). Qualitative Study. National Library of Medicine. *Treasure Island (FL): StatPearls Publishing*. https://www.ncbi.nlm.nih.gov/books/NBK470395/

Thomas, C. et al. (2022). How do study design features and participant characteristics influence willingness to participate in clinical trials? Results from a choice experiment. *BMC Medical Research Methodology. 22.* https://doi.10.1186/s12874-022-01803-6.

Thompson, J. (2022). A guide to abductive thematic analysis. *The Qualitative Report, 27(5), 1410-1421*. https://doi.org/10.46743/2160-3715/2022.5340

Towhidi, G. &Pridmore, J. (2023). Aligning cybersecurity in higher education with industry needs. *Journal of Information Systems Education: Vol. 34: ISS. 1, 70-83*. https://aisel.aisnet.org/jise/vol34/iss1/6

Turk, Ž., Sonkor, M. & Klinc, R. (2022). Cybersecurity assessment of BIM/CDE design environment using cyber assessment framework. *Journal Of Civil Engineering And Management. 28. 349-364. 10.3846/jcem.2022.16682.. Journal of Civil Engineering and Management. Volume 28 Issue 5: 349–364* https://www.researchgate.net/publication/360356458_Cybersecurity_assessment_of_BIMCDE_design_environment_using_cyber_assessment_framework

Ugwu, C. & Eze, V. (2023). Qualitative Research. *International Digital Organization for Scientific Research IDOSR Journal of Computer and Applied Sciences 8(1):20-35, 2023. ResearchGate*. https://www.researchgate.net/publication/367221023_Qualitative_Research

Valkenburg, G., et al. (2020). Making researchers responsible: Attributions of

responsibility and ambiguous notions of culture in research codes of conduct. *BMC Med Ethics 21, 56 (2020).* https://doi.org/10.1186/s12910-020-00496-0

Venkatesh, Viswanath; Thong, James Y. L.; and Xu, Xin (2016) "Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. *Journal of the Association for Information Systems, 17(5).* https://doi.10.17705/1jais.00428 https://aisel.aisnet.org/jais/vol17/iss5/1

Venkatesh, V. et al. (2012). Consumer acceptance and use of information technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly, 36(1), 157–178*. https://doi.org/10.2307/41410412

Venkatesh, V. et al. (2003). Unified Theory of Acceptance and Use of Technology (UTAUT). APA PsycTests. https://10.1037/t57185-000 https://doi.org/10.3846/jcem.2022.16682

Verhage, M., et al. (2024). The Promises of Inclusive Research Methodologies: Relational Design and Praxis. *International Journal of Qualitative Methods, 1–14.* https://doi.org/10.1177/16094069241230407 https://doi.org/10.1371/journal.pone.0261954

Verhoef, P.C. et al. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research, 122, 889-901*.

Villalón-Fonseca, R. (2022). The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity. *Computers & Security, Volume 120, 2022, 102805*. https://doi.org/10.1016/j.cose.2022.102805. https://www.sciencedirect.com/science/article/pii/S0167404822001997

Wallis, T. & Dorey, P. (2023). Implementing partnerships in energy supply chain cybersecurity resilience. *Energies 2023, 16, 1868*. https://doi.org/10.3390/en16041868

Wallis, T. & Leszczyna, R. (2022). EE-ISAC: Practical cybersecurity solution for the energy sector. *Energies 2022, 15, 2170*. https://doi.org/10.3390/en15062170

Walton, S. et al. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems American Accounting Association Vol. 35, No. 1 pp. 155–186*. https://doi.10.2308/ISYS-19-033.

Wang, J. et al. (2022). Research trend of the Unified Theory of Acceptance and Use of Technology Theory: A bibliometric analysis. *Sustainability 2022, 14, 10*. https://doi.org/10.3390/su14010010

Weiss, J. et al. (2023). Changing the paradigm of control system cybersecurity. *The IEEE Computer Society*. https://doi.10.1109/MC.2021.3138231

Werbinska-Wojciechowska, S. &Winiarska, K. (2022). Maintenance Performance in the Age of Industry 4.0: A bibliometric performance analysis and a systematic literature review. *Sensors 2023, 23, 1409*. https://doi.org/10.3390/s23031409

Williams, M.D. et al. (2015). The unified theory of acceptance and use of technology (UTAUT): A literature review. *Journal of Enterprise Information Management, Vol. 28 No. 3, pp. 443-488*. https://doi.org/10.1108/JEIM-09-2014-0088

Wu, M. et al. (2021) Evolution and differentiation of the cybersecurity communities in three social question and answer sites: A mixed-methods analysis. *Plos One*

16(12): e0261954.

Xue, L. et al. (2024). The Unified Theory of Acceptance and Use of Technology (UTAUT) in Higher Education: A systematic review. *Sage Open, 14(1).* https://doi.org/10.1177/21582440241229570

Yan, Y. (2022). The dual foundation of cybersecurity legislation, social sciences in China. *Social Sciences in China, 2022 Vol. 43, No. 3, 4-20.* http://10.1080/02529203.2022.2093065

Yang, M. (2022). Information security risk management model for big data. *Hindawi, Advances in Multimedia Volume 2022*. https://doi.org/10.1155/2022/3383251

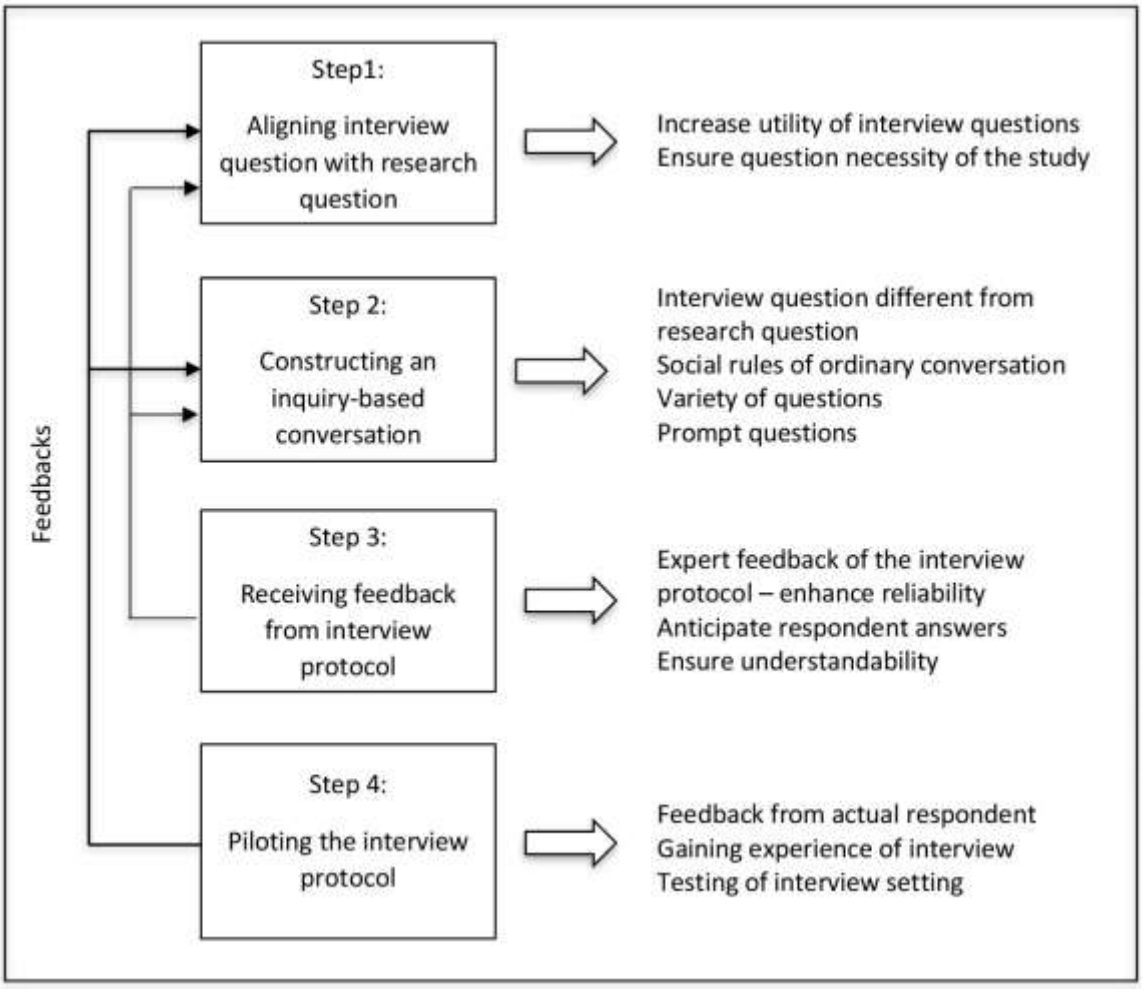
Yoo, C. W. et al. (2020). Is cybersecurity a team sport: A multilevel examination of workgroup information security effectiveness. *MIS Quarterly Vol. 44 No. 2 pp. 907-931/June 2020*. https://doi.10.25300/MISQ/2020/15477

Zadeh, A. H. et al. (2020). Characterizing cybersecurity threats to organizations in support of risk mitigation decisions. *e-Service Journal, Indiana University Press*. https://doi.10.2979/eservicej.12.2.01

Zamberlan, M. & Watanabe, C. (2020). The adoption of an indicator panel in educational management to decision-making support: perception of managers through UTAUT model. *International Journal for Innovation Education and Research. 8. 266-290.* https://doi.10.31686/ijier.vol8.iss6.2411.

Zhang, J. et al. (2023). Survey of technology in network security situation awareness. *Sensors 2023, 23, 2608*. https://doi.org/10.3390/s23052608

Appendix A: Interview Protocol



Appendix B: Letter of Invitation

There is a new study about cloud cybersecurity strategies and controls that may help IT professionals and the general public better understand the benefits and challenges of securing a cloud infrastructure platform. For this study, you are invited to describe your experiences in securing these environments and how users have been made aware of the threats they face when using public and private platforms.

About the study:

- One 20 – 30 minutes phone interview that will be audio recorded (no video recording)
- To protect your privacy, the published study will not share any names or details that identify you.

Volunteers must meet these requirements:

- Cloud cybersecurity professional with at least 3 years of practical experience
- Is resident in the United States.

This interview is part of the doctoral study for Oliver Fontem, a doctoral student at Walden University. Interviews will take place during January 2024.

Please reach out oliver.fontem@waldenu.edu to let the researcher know of your interest. You are welcome to forward it to others who might be interested.