Scientific Research Publishing

Journal of Computer and Communications, 2023, 11, 103-148
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Resilience and Stability in Organizations Employing Cloud Computing in the Financial Services Industry

Daniel Schilling Nguyen, Juliette Sondano

Aspen University, Phoenix, AZ, USA
Email: dans515e@gmail.com

How to cite this paper: Nguyen, D.S. and Sondano, J. (2023) Resilience and Stability in Organizations Employing Cloud Computing in the Financial Services Industry. *Journal of Computer and Communications*, **11**, 103-148.
https://doi.org/10.4236/jcc.2023.114006

Received: January 7, 2023
Accepted: April 25, 2023
Published: April 28, 2023

Abstract

The services and solutions offered by cloud computing continue to grow, just as the number of organizations relying on the service. Cloud computing has become prevalent in the financial services industry, where 83% of financial services institutions identified cloud computing as a primary element of their infrastructure. Although there are specific benefits of cloud computing that organizations rely on such as access to critical services and lower costs, there is the possibility that cloud computing will create costs for organizations. The purpose of the study was to present an intensive review of the benefits and threats by investigating resilience and stability of the organizations in financial services industry that use cloud computing as their primary element of infrastructure. Data collected from the interview was used to answer original research questions, which are: How are organizations in the financial services industry resilient when faced with threats or losses associated with the use of cloud computing in their organization? How do organizations in the financial services industry maintain stability when faced with threats or losses associated with the use of cloud computing in their organization? The study supports the advancement of knowledge by identifying the threats and losses that occur due to the use of cloud computing, and organizations understand common threats and thus implement proper mitigation.

Keywords

Resilience, Cloud Computing, Financial Services Industry

1. Introduction

The services and solutions offered by cloud computing continue to grow, as do the number of organizations relying on them. Accenture (2020) reported that

access to personnel (30%) and lower costs (29%) were the two most frequently selected benefits of cloud computing [1]. Rosati *et al.* (2017) noted the existence of financial benefits from cloud investments in organizations, as cloud computing enables the use of costly services that organizations would not normally be able to afford [2]. Cloud computing has become prevalent in the financial services industry, where 83% of financial services institutions identified cloud computing as a primary element of their infrastructure [3]. Although organizations rely on specific benefits of cloud computing, such as access to critical services and lower costs, it is possible that cloud computing may also create costs for organizations. For example, Sampson and Chowdhury (2021) found that the average monetary cost from a data breach for an organization was $8.19 million, with additional costs associated with meeting regulation requirements, investigation costs, and fines. Several notable providers of cloud computing services such as Google, Amazon, Microsoft, and Salesforce have each experienced data breaches and intrusion problems as providers of cloud services, but organizations remain dependent on cloud computing services as a response to their software, infrastructure, and platform service needs [4]. Thus, understanding how organizations achieve stability and resilience when faced with threats or losses associated with their use of cloud computing is critical.

1.1. Background of the Study

The growth of cloud computing is expected to continue as organizations seek to exploit its benefits. A survey completed by Tata Communications among IT decision-makers in organizations of 500 or more employees found that 85% of respondents believed that cloud computing performs up to the expectations of IT professionals [5]. Cloud computing is responsible for increased speed of technology access, lower delivery times to business partners and clients, and a reduction in delivery time to new markets [5]. Cloud computing technology remains a disruptive technology, as it enables the replacement of rigid software and services licensing models with flexible computing solutions available through the Internet [6].

Organizations utilizing cloud computing can leverage the capabilities of advanced information system technologies that would traditionally only be available to large-sized enterprises and can scale their business with reliance on cloud computing to support their IT activities [6], giving small-to-medium sized enterprises (SMEs) the opportunity to exploit computing technology that traditionally gave large businesses an advantage. There are challenges to implementing and using cloud computing related to its impact on security, governance, and cost, among other issues. These problems are especially serious in the financial services industry, where client data security is a particular concern [7]. These organizations may experience threats, or even losses due to threats, but the capability of firms to remain resilient and stable, even during periods of threats and loss, is critical to their survival. Thus, this study focused on exploring the re-

silience and stability of organizations utilizing cloud computing in the financial services industry.

The financial services industry has specific responsibilities over client data that make considerations related to cloud computing more complex. The case of Capital One is a key example [4]. In 2011, Capital One was one of the earliest financial services organizations to adopt cloud computing. The organization had a contract with Amazon Web Services for cloud computing services [4]. When a breach occurred that made the personal financial information of Capital One clients available to intruders, Capital One became liable for $80 million in civil penalties. The case set the standard for the responsibilities of organizations in cloud computing services agreements, where the cloud computing vendor would become responsible for the security of the cloud and the customer was responsible for the data in the cloud [4].

The financial services industry also includes specific regulations that institutions may have difficulty addressing, particularly when the organization operates across multiple jurisdictions [4]. Celner (2021) noted that although regulatory compliance issues can create challenges for multinational or global financial institutions, organizations specializing in cloud solutions can focus on support organizations by responding to compliance issues as they emerge. While advantages exist for financial services organizations, threats to stability can challenge the resiliency of the organization when utilizing cloud computing [8]. Reliance on the cloud makes the organization as vulnerable as their third-party vendors for cloud services. Organizations must be alert to these threats and challenges by developing proper security processes, training, and technical countermeasures in order to remain resilient. This study explores how organizations remain resilient and maintain stability when faced with threats or losses associated with the use of cloud computing.

Although cloud computing holds immense benefits for organizations seeking information system capabilities that would traditionally be cost prohibitive or difficult to implement and maintain, organizations implementing cloud computing must also accept some risks do not present in their legacy systems. The results of a survey involving technical professionals and the management in organizations utilizing cloud computing showed that security is the most frequently named challenge, with 81% indicating that security is a challenge to enterprise cloud computing usage [9]. Organizations implementing cloud computing-based solutions for information system capacity or capability issues are somewhat dependent on the vendors for these services, and the theft or damage of data can occur because of weaknesses in third-party systems. Organizations in several industries, such as the financial services industry, are especially dependent on the security of their data because they are responsible for their clients' private financial data [10].

The Federal Financial Institutions Examination Council has provided guidelines on the use of cloud computing services by financial institutions, focusing on the issue of risk management practices. They noted that financial services in-

stitutions must consider business continuity planning as a critical aspect of how they conduct risk management. Thus, it is critical to explore institutions' resilience and stability of financial services in the face of threats or losses associated with the use of cloud computing, practical knowledge, and best practices to better understand how financial services organizations move forward from such threats.

1.2. Research Questions

1) How do organizations in the financial services industry remain resilient when faced with threats or losses associated with the use of cloud computing in their organization?

2) How do organizations in the financial services industry maintain stability when faced with threats or losses associated with the use of cloud computing in their organization?

1.3. Rationale for Research Design and Methodology

The research method and design for the proposed study was qualitative and descriptive. A qualitative research methodology was selected as the preferred method for this study because the business problem involves understanding how organizations maintain stability and remain resilient when faced with threats or losses associated with their use of cloud computing. The business problem involves exploring the processes businesses would select in response to a problem. A qualitative research methodology enables an understanding of the lived experience of individuals. In the proposed research, the lived experience of IT professionals was explored to understand the process of maintaining stability and remaining resilient. A quantitative method was not appropriate to this research. Quantitative methods involve understanding probabilities, counts, and other statistical information. Therefore, numerical data would be inappropriate in this context because the data could not support developing knowledge related to the experience of IT professionals with cloud computing.

Thus, the most appropriate research design for this study was a descriptive design. A phenomenological research design was considered, as phenomenological research focuses on understanding the lived experience of individuals [11]. But as the existence of threats and losses through cloud computing is a phenomenon, a phenomenological design was deemed inappropriate because the research questions are associated with describing how organizations achieve something during periods of threats and losses, namely stability and resilience. The business problem involves exploring how organizations in the financial services industry maintain stability and achieve resilience when faced with threats or losses associated with their use of cloud computing. Thus, a descriptive design was deemed the most appropriate research design for the proposed study.

The qualitative, descriptive design in this study involved the use of a structured questionnaire [12] to collect data from participants. Participants were se-

lected using a purposive sampling approach, which enables collecting data from specific individuals. The participants in this study were individuals who work as IT professionals in the financial services industry whose organizations have experienced threats or losses. The survey questions were designed to understand how the organization-maintained stability and achieved resilience. Institutional theory and resilience theory was used as a theoretical lens through which to design the survey questions. A sample size of 15 participants was used for data collection.

A reflexive thematic analysis approach was used for data analysis [13]. Reflexive thematic analysis involves coding as the basis for data analysis and the development of themes [14]. At the conclusion of each structured questionnaire, the data from SurveyMonkey was transcribed into a text document. The text document was then coded with initial codes. Once the point of redundancy was reached in coding the structured questionnaire, the point of saturation was assumed to have been reached. The data was then coded formally and explored to develop themes, which were then interpreted to respond to the research questions.

1.4. Definition of Terms

Cloud computing. The use of computer remote servers networked through the Internet to manage, store, and process data rather than through local servers or computers [15].

Losses. A reduction in some sort of resource for an organization [16].

IT professional. An individual responsible for working with information technology [15].

Resilience. The capacity of an entity to recover from damage [15].

Stability. The state of an entity as not disturbed [17].

Threats. The potential of danger for an entity [17].

1.5. Assumptions, Limitations, and Delimitations

A crucial assumption made for this research was that the responses by the participants in structured questionnaire were completely truthful and honest, as suggested [18]. The IT professionals selected to participate in this study were individuals with experience working in the financial services industry who have experienced losses or threats associated with their organization's use of cloud computing. The IT professionals selected had accurate knowledge of their lived experience [18] and no reason not to be truthful. The validity of the research, in part, relied on the trustworthiness of the data, and the truthfulness of participants was the factor impacting trustworthiness. Therefore, the assumption of the truthfulness and honesty of participants remains a key assumption. The strategy for mitigating the likelihood of participants not being truthful was to assure them that their survey responses would be confidential and that no names or other identifying information would be used.

It was also assumed that the experience of participants was in-depth enough to support their capacity to respond to structured questions with enough insight into how the organization was resilient and maintained stability following a threat or loss associated with its use of cloud computing. The individuals participating in the study were IT professionals, so their experience should be tied to their organization's response to the problem. The assumption is that the participants in this proposed study were a part of the response to threat or loss or were in a position to observe their organization's response.

Another assumption is associated with the study's conceptual framework, one that includes both institutional theory [19] [20] and resiliency theory [21], both of which remain relevant to research involving organizations. The assumption is that institutional theory and resiliency theory are appropriate theories to use in designing the structured questionnaire in this study. The findings supported responding to the research questions of the proposed dissertation providing the theoretical framework was correct and accurate; however, the findings did not support responding to the research questions if the framework was not correct for this study. At the conclusion of the survey, participants were asked for additional feedback regarding their experience with threats and losses associated with the use of cloud computing to determine whether the theoretical framework enables the robust collection of data associated with the research questions.

A key limitation of this research was associated with the selected sampling method. The study had small sample size of 15 participants, although the sample changed depending on when the point of data saturation was reached. Still, the smaller sample size and the nature of the qualitative data collected support the limitation of this research where it was not generalizable beyond the population of IT professionals working in the financial services industry in the U.S.

Another limitation of this study was that the research design did not enable drawing causal inferences. The research method and design for this study was qualitative and descriptive. A qualitative and descriptive research methodology and design do not enable one to determine cause or cause and effect relationships. Therefore, the study's findings could have explanations other than those expressed in its findings and conclusions.

Bias presents yet another limitation of this study. Qualitative research includes the risk of researcher bias influencing the researcher's findings or conclusions. Flyvjberg (2006) noted that bias in qualitative research is difficult to reduce because of the inductive nature of qualitative research [22]. A tool for reducing bias in qualitative research is using a reflexive journal, which allows researchers to keep track of decisions and to reflect on their rationale and understanding of what the decisions meant their research [13]. Thus, a reflexive journal was kept in order to reduce the existence of bias when interpreting the study's findings.

This research also has several delimitations. The first was the study's location. The location selected for the proposed study was the United States. The size of firms operating in the financial services industry makes it difficult to reduce the location to a small regional area. However, selecting a small regional area may be

an invalid decision, given that these firms operate in different countries and that what is relevant is understanding the experience of their IT professionals. Another delimitation was the industry selected: the financial services industry. The financial services industry was selected because of the intensity of the concerns related to financial data and the danger that threats and losses pose for consumers.

2. Literature Review

2.1. Contextual Background

Cloud computing is a disruptive technology that organizations across several industries rely on to support greater technological capacity and access to a diverse network of digital tools. Cloud computing is an information system networking strategy that involves an organization relying on larger, centralized information systems that offer greater data storage or information system power [23]. The advantage of cloud computing is that an organization need not take responsibility for the software or hardware in the cloud computing schema, as the software is offered by a third-party vendor [23]. Thus, the organization is able to reduce its association with data storage and computing power by relying on the third-party vendor sharing resources [23]. Therefore, cloud computing offers an organization the opportunity to minimize expenses while optimizing their access to storage, power, or other advantages offered by vendors.

While the concept of cloud computing has existed for several decades, the capability for cloud computing to offer advantages or opportunities for organizations has grown only in the last decade. The concept of cloud computing was initially articulated at a time when the Internet was still emerging [15]. Remote job entry was among the first applications of technologies that would become modern cloud computing practice. Remote job entry was a practice whereby several users would share the same information system resources [15] [23]. Advances toward cloud computing were then supported by the emergence of virtual private networking services in the 1990s. The initial conceptualization, through the design of ARPANET and CSNT, identified the design of the Internet as similar to that of a cloud in terms of how entities could connect through information communication technology, particularly phone lines. The concept continued to be refined throughout the 1990s [15] [23]. However, conceptualizing the cloud was still at a point where scholars and professionals were identifying the advantages of the cloud for organizations. Telescript was the first recognized instance of the emergence of the virtual service concept. While limited, the service was the first step in establishing cloud computing as a service. As the Internet became increasingly robust in the 2000s, services emerged to support the modern practices of cloud computing, whereby the focus was placed on offering organizations the ability to use storage, power, and other services through their data centers [15]. Modern cloud computing solutions offer cost savings and access to services that can result in smaller firms becoming more competitive with larger

firms.

Cloud computing offers an advantage to clients because of the different options available in terms of services offered and how these are deployed. Cloud computing offers several different service models, depending on the nature of a client's needs based on the service-oriented architecture of the design of cloud computing models [15] [23]. Specifically, there are three distinct models of cloud computing: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [13] [23]. Each model of service represents a different level of client dependency on a cloud computing service. Clients never take possession of the software, platform, or infrastructure, but access it through cloud computing [15] [23]. With SaaS, the client is only dependent on the service provider for cloud computing at the application level. Email, games, or communication tools are examples of applications delivered through the cloud through SaaS [15] [23]. Through PaaS, the client is dependent on the cloud computing service provider for platform-level service delivery. Some examples include databases, development tools, and webservers. In IaaS, the client is dependent on the delivery of infrastructure characteristics through the cloud. Examples include virtual machines, storage, and servers. Access to these services allows organizations to access an information system framework that would otherwise be cost-prohibitive [15] [23]. Thus, substantial advantages can be obtained through cloud computing.

While cloud computing is a valuable service, there are unique threats that do or do not exist or are not as prevalent with legacy systems. Mlitz (2021) presented survey data collected from technical executives, practitioners, and managers using cloud computing strategies [9]. The most frequent challenge in Q4 2020 was security (81%), followed by the cost for cloud computing (79%), with governance, a lack of resources, and compliance each reported as a challenge by 75% of respondents [9]. Security remains a problem for cloud computing, as insecure interfaces, data leakage, and hardware failure are frequent problems for clients using cloud computing [9]. These threats exist because when the organization is a client using the services of a third party in possession of the hardware used in the cloud, the security, privacy, and performance of the services offered remain dependent on the service provider. That service provider could change or delete data from a client's account or share client data with other organizations. There are solutions to the problem of security and privacy, such as data encryption [15] [23]. However, maintaining the encrypted files can become difficult for organizations. Another solution to the privacy issue is identity management systems, which limit the types of entities that could gain access to a system and the type of data they have access to. Still, creating a security protocol in cloud computing can lead to additional costs and complexities for the organization, which exacerbate several issues noted by Mlitz (2021), namely security, spending on cloud services, and expertise [9]. Thus, while cloud computing offers certain advantages, the organization is also responsible for dealing with its challenges.

2.2. Conceptual Framework

The conceptual framework for this study includes two theories: institutional theory and resiliency theory. These theories enable one to explore how organizations in the financial services industry maintain stability and achieve resilience when faced with threats or losses associated with their use of cloud computing, based on the perceptions of IT professionals working in the industry. Institutional theory was included in the theoretical foundation of the study because of its association with how organizations interact with their environment and the resiliency of organizations when facing adversity from their environment [19] [20] [24]. Resiliency theory was included in the theoretical framework of the study because of the role of resiliency in institutional theory [19] [20] [24] and resilience theory's association with how organizations orient themselves, move forward, and adjust to challenges [19] [20] [24]. This section of the literature review describes these theories and how they fit together within the study's theoretical framework. Seminal research related to these theories is included in this description of the theoretical foundation of the study.

Institutional theory was selected as a part of the theoretical framework for this study because of it involves understanding how resiliency and stability emerge from the structure, policy, routine, and guidelines for social behavior in organizations [19] [20]. Scott (1995, 2004) considers resilience a necessary characteristic of institutions. Resilience, within the context of institutional theory, supports the continuity of a business. For an organization to survive, its elements must conform to the current structure and characteristics of the surrounding environment [19] [20]. In the context of how organizations in the financial services industry maintain stability and achieve resilience when faced with threats or losses associated with their use of cloud computing, the theoretical foundation is associated with environmental factors such as policies surrounding how financial institutions manage data in cloud computing and the responsibility of financial institutions to their clients regarding threats and losses, the economic impact of using cloud computing regarding threats and losses, the technological capabilities associated with the cloud, and the extent to which threats and losses can occur.

Another critical element of institutional theory is how the institution's environment influences the development of formal structures within an organization. Meyer and Rowan (1977) noted that the influence of the environment on institutions is often greater than the influence of market pressures on how the formal structure of organizations emerges [25]. The formal structure of organizations within an industry can then influence the adoption of standards and how competitors in the industry adopt structure and form, even though the economic impact of adopting some structural facets is negative due to the perception that adopting structural aspects will contribute to the legitimacy of the new organization [25]. The formalization of leading organizations in an environment will then influence the formation of roles and protocol for new competitors and

smaller entities in a market, as other firms entering a market emulate the structure of organizations in the industry. Meyer and Rowan (1977) refer to these as institutional myths, which are accepted as axiomatic within their industrial environment [25]. The extent to which standards and common norms emerge among competitors in the industrial environment is a characteristic of institutional theory that wields substantial influence on organizational practices. This characteristic is also a crucial element of this study's theoretical framework: while organizations must be prepared for threats and losses, the amount of preparation within the environment can influence how stability and resilience are maintained.

The formation and acceptance of institutional myths within an industry can result in organizations accepting organizational inefficiency and difficulties associated with preparing for organizational challenges. DiMaggio and Powell (1991) also discussed the issue of institutional pressures onset by the formation of institutional myths within an environment, identifying three distinct pressures placed on organizations to accept the legitimacy of institutional myths in how their organization form and evolve: coercive pressures, mimetic pressures, and normative pressures [25]. Coercive pressures in institutional theory are associated with forces such as legal mandates and the influence of the dependency on other organizations. Mimetic pressures are associated with the pressure that organizations experience in replicating the structure of successful organizations due to uncertainty in the institutional environment. Normative pressures are associated with the degree of homogeneity that exists due to the similarities in approaches between associations and groups that are absorbed by the organization based on their recruiting and hiring practices [25]. These pressures are responsible for the degree of institutional isomorphism that emerges in the environment.

Institutional theory remains a critical element in understanding how organizations form and address challenges or threats within their environment. In discussing institutional theory, Meyer and Rowan (1977) focused on how it addresses change in organizations [25]. The conceptual discussion by Abbott (1991) included identifying distinct dimensions of institutions that were relevant to change and to practicing stability and homogeneity [25]. The existence of homogeneity across institutions in an environment was discussed by Meyer and Rowan (1977), who suggested that organizations adopt similar processes [25]. DiMaggio and Powell (1991) also supported homogeneity, as the three pressures discussed focused on pushing institutions toward accepting the same structural elements [25]. However, although stability was not mentioned, it remains an important element of institutional theory, with Barley and Tolbert (1997) acknowledging that organizational stability emerges from organizational practices that are formed based on practices across industries [25]. Thus, exploring resilience and stability in the face of threats associated with the use of cloud computing in the financial services industry requires the use of institutional theory as a part of the study's theoretical lens. The inclusion of resilience theory can enable further exploration of the problem.

The inclusion of resilience theory as a theoretical framework for this study was influenced by the characteristics of institutional theory related to the capacity of institutions to remain resilient and by the focus of the study on how organizations in the financial services industry maintain stability and achieve resilience when faced with threats or losses associated with their use of cloud computing. Scott's (1995) description of institutions as social structures with "a high degree of resilience" (p. 33) supports the inclusion of resilience theory in the study so that it can better describe how institutional resiliency is achieved in financial institutions faced with loss or threats [19]. Resilience theory identifies the need for firms to maintain a capacity for resilience, given the dynamic nature of the environment that surrounds them, where unexpected threats and challenges often occur [26]. Resilient firms will emerge from a challenge or crisis stronger than they were when they encountered the crisis [26]. Thus, resilience theory can promote an understanding of how financial services organizations facing threats or losses stemming from cloud computing became stronger following those crises.

Resilience theory in organizations addresses the importance of organizations addressing unexpected situations in ways that support the improvement of the organization following a crisis. Barley and Tolbert (1997) and Lengnick-Hall *et al.* (2011) discussed resilience in organizations, noting that firms must develop a resilience capacity in order to react to and capitalize on unexpected events [27] [26]. Resilience theory supports organizations moving beyond being flexible, agile, or robust. Lengnick-Hall *et al.* (2011) noted that resilience differs from flexibility, agility, and robustness in that it supports the achievement of positive change for the organization stemming from a negative event [26]. Although flexibility is a beneficial characteristic for organizations, it is limited because it focuses on an organization's ability to adjust to changes in the environment [27] [26]. Agility was noted as another beneficial characteristic for organizations, albeit limited in that it focused on the capacity to quickly identify opportunities, change direction, and avoid problems [26] [27]. Robustness differs from resilience, as it is associated with the capacity of an organization to maintain functionality even when disruptions occur [26] [28]. Resilience significantly differs from these characteristics because it addresses the issue of adaptation to the environment, whereby an organization learns how to improve through adversity. Thus, organizational resilience remains a critical element in the response by financial institutions during threats to or losses for the organization.

Through organizational resilience, an organization can absorb changes and move forward stronger than it had previously been. Xiao and Cao (2017) and Annarelli and Nonino (2016) discussed the concept of organizational resilience, noting that it was focused on how organizations bounce back from environmental changes and adapt in ways that result in the organization becoming stronger [21] [29]. However, the conceptualization of resilience has been the source of some disagreement by scholars concerning at what point the organization should intervene to adjust to disruption and whether organizational resi-

lience is an issue of correction or detection. Annarelli and Nonino (2016) specifically emphasized the role of strategic awareness and knowledge of the possibility of environmental changes that could create internal or external shocks for management [29]. Lengnick-Hall *et al.* (2011) and Xiao and Cao (2017) emphasized the capacity of an organization to absorb environmental changes while developing a response and engaging with changes in order to capitalize on problems caused by disruptive surprises [21] [24]. In their conceptualization of organizational resilience, Xiao and Cao (2017) specifically included a model that highlighted the influence of organizational learning as part of how organizational resilience can occur, whereby the organization improves through changes to structure, improvisation, reliance on social capital for solutions, and attention to the failures of the organization, before moving toward recovery [21]. Thus, the organization can improve through reliance on organizational resilience.

The inclusion of both institutional theory and resilience theory in the framework of the proposed research was based on the importance of institutions coping with unexpected situations in innovative ways, which can result in growth and improvement of the positioning of the organization. Institutional theory describes the environment as having an impact on the structure and direction of organizations [24] [26]. On the other hand, resilience theory addresses how organizations adapt to the environment or environmental changes that challenge the success of the organization [24] [26]. Institutional theory enables us to better understand how organizations address threats and losses within the context of the conventions in their environment [24] [26], while resilience theory helps us understand how organizations move forward with a stronger positioning as a result of their experience and reaction to the environment [24] [26]. Stability remains an important element for organizations as they seek homeostasis in a dynamic environment [19] [20]. However, the organization must continuously improve. Exploring how organizations achieve resilience in a scenario where they face threat or loss can contribute new knowledge that can fuel their improvement. Thus, the inclusion of both institutional theory and resilience theory in the study's theoretical framework can contribute practical knowledge that in turn can bolster the success of organizations in the financial services industry.

2.3. Related Studies/Literature Review

Studies abound on topics related to the proposed research. However, few of them directly address how organizations in the financial services industry maintain stability and attain resilience when faced with threats or losses associated with their use of cloud computing. From 2014 to 2019, the number of cyberattacks increased a dramatic 67% and their cost increased 72%, with an average cost of $13 million dollars per attack [30]. Schuh (2019) noted the importance of cyber resilience, based on the National Institute of Standards and Technology's (NIST) Special Publication 800-160 [31]. The NIST publication identified cyber resilience as involving the capacity for organizations to anticipate, withstand,

recover from, and adapt to adverse conditions [31].

Research has examined the role of organizational resilience during the cyberattack lifecycle. Anderson *et al.* (2020) and Bouwens and Stafford (2019) explored the characteristics of resilience organizations require during the cyberattack lifecycle [30] [32]. They noted that organizations generally have some obligation to maintain security against cyberattacks because of the possible loss of consumer data. The General Data Protection Regulation of the European Union and the California Consumer Privacy Act in California are examples of legislation that have created an obligation for organizations to manage data and prevent cyberattacks (Bouwens & Stafford, 2019). Anderson *et al.* (2020) and Bouwens and Stafford (2019) also noted that while organizations continue to invest in cyber security to prevent cyber intrusion, advanced persistent threats continue to threaten organizations [30] [32]. Human factors can play a critical role in the success of an organization related to resilience in cyber security incidents [30] [32]. Human error is the most critical threat of all during cyber security incidents, while it also remains a more complex issue to address in terms of resilience [30] [32]. Therefore, the current research focused on understanding how organizations that remain resilient following cyber security threats can maintain some focus on the human elements of these threats.

The objective of organizations in addressing cyber threats is to mitigate the likelihood of successful attacks, but also to be resilient when attacks are successful. Galinec and Luic (2019) and Schuh (2019) noted that organizations must accept that all systems contain vulnerabilities, and that organizations must design information systems that are highly resilient to cyber threats [31] [33]. They also discussed the issue of cyber resilience, noting that digital security should play a role in establishing cyber resilience in organizations. Digital risk management is a critical performance issue for organizations that must consider how business leaders make decisions relating to the resilience of their organization's cyber security schema [31] [33].

The conceptualization of the role of cyber resilience by Galinec and Luic (2019) and Schuh (2019) support the importance of an emphasis on technical design factors to assist the systems in the organization in overcoming the challenges presented by threats and losses [31] [33]. However, their discussion and those of Galinec and Luic (2019) and Schuh (2019) failed to focus on the human factors associated with organizational resilience in the face of threats and losses [31] [33]. Hence, there remains a gap whereby organizational factors outside the technical design of the organization address problems associated with resilience in cyberattacks.

The concept of resilience in information systems also extends to how systems and smart devices are designed to support the resilience of infrastructure in light of threats and disruption. Thorisson *et al.* (2019) discussed the issue of the resilience of critical infrastructure, noting that while technologies offer advantages and efficiencies to individuals, there are several threats that devices such as smartphones, identification devices, sensors, and actuators experience in organizations

[34]. Thorisson *et al.* (2019) explored this problem from the standpoint of the technical design of devices, rather than examining how individuals in the organization support the achievement of resilience in an organization [34].

3. Methodology

3.1. Research Methodology

The research method and design for the proposed study is qualitative and descriptive. A qualitative research methodology was selected as the preferred method for this study because the business problem involves understanding how organizations maintain stability and remain resilient when faced with threats or losses associated with their use of cloud computing. The business problem involves exploring the processes businesses would select in response to a problem. A qualitative research methodology allows us to understand the lived experience of individuals. In the proposed research, the lived experience of IT professionals was explored in order to understand the process of maintaining stability and remaining resilient. A quantitative method would not be appropriate for this research, as quantitative methods entail understanding probabilities, counts, and other statistical information [35].

Thus, numerical data would be inappropriate in this study because such data could not support developing knowledge related to the experience of IT professionals with cloud computing. Mixed methods involve mixing qualitative and quantitative research within different stages of the research process [36]. Thus, combining idiographic and nomothetic approaches would also be inappropriate because the study details only a small sample of IT professionals. A mixed method is also difficult to conduct by a single researcher [35], as the research must concurrently apply more than one approach. Guetterman (2020) notes that researchers choosing mixed method research must study multiple approaches and methods and learn how to mix them [35]. According to O'Hanlon (2018), mixed method is time consuming due to content duplication [36].

3.2. Design of the Study

Although there are several research designs, a descriptive design was deemed the most appropriate one for this study. A phenomenological research design was considered, as phenomenological research focuses on understanding the lived experience of individuals [18] and the existence of threats and losses through cloud computing is a phenomenon. However, a phenomenological design was deemed inappropriate because the research questions involve describing how organizations achieve something during periods of threats and losses, namely stability and resilience. A case study design was also considered. According to Heale & Twycross (2017), case study designs are appropriate when the focus of a study is on understanding a process [37]. However, a case study would not be appropriate because it would require locating one or several organizations experiencing threats or losses based on their use of cloud computing and locating an

organization currently experiencing such a problem would not be feasible. An ethnography design would also be inappropriate, as ethnographies involve describing customs and cultures [12]. A descriptive design was deemed the most appropriate research design associated with a qualitative methodology because it involves describing behaviors in situations [12]. The business problem involves exploring how organizations in the financial services industry maintain stability and achieve resilience when faced with threats or losses associated with their use of cloud computing. Thus, a descriptive design was deemed the most appropriate research design for the study.

3.3. Sample and Population

The population for this research included IT professionals working in the financial services industry. Based on statistics from banks, there were 8.91 million individuals working in financial services as of November 2021, and 34% working as digital talents to some degree. The total number of individuals in the population for this study was 15. A purposive sampling strategy was used to determine the individuals included in the study. The inclusion criteria for participants were IT professionals working in the financial services industry. The exclusion criteria were that only IT professionals who had worked for their organization during a period of threat or loss onset by the use of cloud computing were included in the study.

A purposive sample selection per the mentioned inclusion and exclusion criteria was performed using the third-party service User Surveys. User Surveys is a sample selection service that connects professional and academic researchers with individuals for qualitative research. User Surveys has a database of over one million Americans over the age of 18 that are interested in participating in research surveys for a fee. Once User Surveys recruits individuals that meet the inclusion criteria and do not meet the exclusion criteria for the study, the researcher will use the User Surveys graphic user interface to send the informed consent letter to each potential participant and, once consent is obtained, the surveys will be scheduled. The researcher will send a LinkedIn link for the agreed-upon date and time to each study participant, independently and not using User Surveys. Because User Surveys samples individuals from across the United States and not from a specific organization, site authorization is not valid insofar as each individual participant will work for different organizations and take the surveys on their own time from their homes.

The pre-determined number of individuals to include in this study is 15; however, there may be more or fewer participants, depending on whether the point of data saturation is reached. The point of data saturation is reached when data collection becomes redundant [22]. Thus, while 15 was the estimated number of participants considered necessary to reach the point of saturation, that number did not influence the actual number of participants needed for the study. The means of communication with participants were via email and LinkedIn. A con-

sent form and letters of invitation (see **Appendix A** and **Appendix B**), purpose, method, and the introduction to the background of the study were included as suggested by Nguyen (2016) [18].

3.4. Instrumentation and Data Sources

Two instruments were used in this study for the purpose of data collection. The first instrument is a demographic survey (see **Appendix C**) that emailed to participants recruited via User Surveys. The survey was implemented using SurveyMonkey and only collected details on personal profile characteristics, which included participants' gender, age, ethnicity, income level, and years of job experience. The data was then used to develop a profile table listing the participants' characteristics, including the counts and frequencies for each characteristic listed in the survey instrument.

The primary investigator of the study was the second research instrument. The primary investigator is considered an instrument [7] in this study because of their role in reading survey questions, but more importantly in determining how to respond to participants regarding follow-up questions. The surveys are structured, meaning that additional questions might possibly become a part of the survey process. Thus, the primary investigator must be considered an instrument. Regarding the validity and reliability of the primary investigator, a reflexivity journal was used in the survey process to support constraining bias and addressing possible bias when compiling the study's findings. The reflexivity journal can support reflection on changes or follow-up questions during the survey process.

3.5. Validity and Reliability

Trustworthiness is how validity and reliability are assessed in qualitative research. There are four characteristics of trustworthiness in qualitative research: credibility, transferability, confirmability, and dependability, each of them determining whether research findings should be trusted.

The first characteristic of trustworthiness is credibility, which is associated with confidence in the truthfulness of findings [38]. There are a few strategies used in this study that support credibility [39]. One is associated with the design of the survey questions. Once designed, the questions were analyzed by experts in the field to confirm they were consistent with the study [39]. Another method that was used to establish credibility was the use of pilot study participants. Two pilot study participants were included in this research to test the use of the survey questions in a real setting without including actual participants. The last element for establishing credibility involved the use of member checking [40]. Participants were asked to review their responses and the write-up of the study to determine whether the interpretation was accurate.

The second characteristic of trustworthiness is transferability, which is associated with the degree to which study findings could be applicable in other stu-

dies [38]. The transferability of the study results was determined based on the characteristics of participants [41]. Participants were IT professionals working in the financial services industry. Personal profile characteristics are characteristics that could possibly influence the study's findings. However, they are not part of the characteristics for inclusion or exclusion in a purposive study. Collecting data on profile characteristics and on individuals filling one role in one industry enables one to determine the transferability of the research across different organizations.

The third characteristic of trustworthiness is confirmability, which is associated with the extent of neutrality in the findings of a study [38]. Confirmability, in part, deals with the issue of bias in research and the extent to which possible skews in interpretation could occur [42]. One method used to reduce bias in this study was to use member checking as part of the data analysis procedures. Member checking supports a reduction in bias by giving the survey participants in a study the opportunity to review their responses to determine whether the interpretation of survey question responses was consistent with participants' responses. Confirmability is also assisted by the use of a journal. A reflexivity journal was utilized, and the primary investigator reflected on the journal when interpreting the data.

The fourth and last characteristic of trustworthiness is dependability, which is associated with the extent to which the completed research could be replicated by another researcher and with another researcher producing similar findings [38]. Dependability focuses on establishing consistency between the current study and other research. Dependability in this study was established through the consistency of data collection activities [42], as the same procedures were used for each survey. There was no need to change the procedure or other elements of the survey protocol; had there been, then prior surveys would have been discarded and only surveys completed following the change would have been included in the study.

3.6. Data Collection

The procedures for data collection in this study began with a request to access IT professionals to take a structured questionnaire and concluded once the point of data saturation had been reached. Data collection in this study included collecting survey data from participants related to their profile characteristics and structured questionnaire data. Data was collected and an iterative analysis of the qualitative structured questionnaire data was performed to determine when the point of data saturation, the point when further data collection would be redundant, had been reached. Braun & Clarke (2014) suggest structured questionnaires as a method of collecting data for thematic analysis [14] [43]. Once all data was collected, data analysis began.

Data collection was carried out by contacting organizations whose workers would be a good fit for the study. The organizations from which participants

were selected are financial services organizations known to have experienced losses or threats due to their use of cloud computing. The specific workers that were selected to participate in the study are IT professionals. Human resource managers in the selected organizations were contacted by email. The email addresses of human resource managers for the selected organizations were located using the organization's website or by calling the organization to obtain the Human Resource department's email address. Emails were sent to organizations describing the purpose and nature of the study, along with a copy of the dissertation proposal, as approved by the dissertation committee and the IRB of Aspen University. The emails requested that Human Resources forward the researcher's email to IT professionals working in the organization's financial department. An alternate means for recruitment was LinkedIn. Once permission was obtained from the LinkedIn group project manager, a pool of qualifying participants was recruited through the LinkedIn platform.

When approval was received to contact members of the organization for the purpose of this study, the participants were contacted via email, direct approach, or LinkedIn. An email script was used to query IT professionals about their interest in participating in the study. The email contained details about the research and the responsibilities of participants. It also included a copy of the dissertation proposal for the study. If the IT professional expressed interest in participating in the study, a copy of the informed consent form (see **Appendix A**) was sent to the participant, with instructions to sign the form and return it to the primary investigator prior to the survey. Once the informed consent form was received, a link to a SurveyMonkey survey was then sent to the participant for the purpose of collecting data related to their profile characteristics.

3.7. Data Analysis Procedure

Informal data analysis was completed following each structured questionnaire. Once the text data was transcribed, informal coding was completed. The informal codes were used to determine whether the point of data saturation had been reached. Saturation was determined based on whether the responses from participants became redundant. Once saturation was reached, formal coding began. The formal data analysis procedure began by gathering the collected data and organizing it for analysis. Data collected to describe the profile characteristics of participants was organized and examined using Microsoft Excel 2020. Data collected for the purpose of responding to the study's research questions was imported into MAXQDA.

The data imported to Microsoft Excel 2020 was examined to measure frequencies for the demographic characteristics collected in the study. Percentages were used to describe the profile characteristics of survey participants. The findings were presented in the write-up of the study using tables, after which the formal analysis of qualitative data began, using Braun and Clarke's (2006) process for reflexive thematic analysis [14] [43] [44].

3.8. Reflexive Thematic Analysis

The reflexive thematic analysis process includes six phases, beginning with informal coding and concluding with member checking. The first phase of reflexive thematic analysis occurs during the process of data collection. Each survey is coded with start codes and notes where data from each survey was read and re-read to determine when saturation had been reached and redundancy and patterns became evident [43]. The reflexivity journal was used to collect the start codes, the informal descriptions of codes, and the source of the code. The use of informal coding and robust notetaking is also supported by Saldana (2015) [45].

The second phase of data analysis began after the completion of data collection and ended once the point of data saturation had been reached. This second phase involved the creation of initial codes. Unlike the informal codes formed in phase one, initial codes were developed to arrive at comprehensive codes focused on how the data can respond to the research question. Phase two involves the creation of initial codes to document potential patterns in the data. Saldana (2015) supports reflection on the informal codes created by the primary investigator when creating the initial codes [45]. The use of coding during phase two is essential because the robust, raw qualitative data is collapsed into codes and the data is reduced for efficient analysis [14]. During this second phase of data analysis, the reflexivity journal is a useful tool to support further work in future phases. The journal includes a reflection on the combination of codes and how the codes are related.

The third phase of reflexive analysis involves the preliminary development of themes from the data. This phase of data analysis involves combining codes into preliminary themes used to describe the data. The focus of this phase is on the creation of candidate themes that can be used by the primary investigator while exploring the data. The preliminary theme must be described with an explanation of what the themes mean [44]. The primary investigator must also provide details about characteristics that are missing from the analysis and what does not appear to fit in the data. The reflexivity journal is used at this phase as a tool to interpret the codes in order to create themes within data.

The fourth phase involves a reflection on how the themes support the data and theory. This phase requires that the researcher review the preliminary theme to determine whether themes are consistent with the data and the framework of the study. The primary investigator must review the themes to determine how well they support the data and their consistency with the theoretical perspective of the dissertation. At the conclusion of the fourth phase of reflexive thematic analysis, there should be an understanding of the patterns among themes [13]. Where there appears to be incomplete data, the primary investigator must continue to review the data to determine if there is anything missing from the analysis. The reflexive journal was used in this phase to collect notes related to how the themes should be understood and how the patterns support understanding the data. This phase concludes by determining the patterns within themes and

with an accurate narrative involving the data.

Phase five involves a comprehensive description and understanding of the data. It involves a review of the findings and a consideration of what the themes mean for understanding the data. Each theme selected was defined, with an articulation of what is novel from the findings in the data. This fifth phase concludes by determining how themes support understanding the data collected for the study [43]. The reflexive journal was used to establish what each theme means.

The sixth and last phase involves writing up the findings and the completion of member checking to ensure that the interpretation of the data was consistent with the findings of the primary investigator. This final phase involves describing the findings and completing checks that ensure the quality of the data. It also involves understanding the themes that best describe the data and is responsible for contributing to an understanding of the phenomenon [46]. The conclusion of phase six includes the findings. Member checking is also completed during this phase. The participants were asked to give their assurance that the interpretation of the findings was accurate. Once assurance was received from survey participants via member checking, Results and Discussion was written.

3.9. Limitations and Delimitations to the Methodology and Design Summary

There are some limitations and delimitations associated with the methodology and design of this study. A limitation associated with the method of this study is that the data collected was not measured based on any type of central tendency or variance, as the data involved the interpretation of the lived experience of the participants. Another limitation of the research is that the study involved describing the conditions and the phenomenon. A delimitation of this research is associated with the use of computer-mediated communication to support data collection. The use of LinkedIn for data collection is a delimitation, as it is the selection of a technological tool that can support communication using audio and video technology. An associated delimitation within the study design is that only text data was analyzed. Saldana (2015) noted the importance of using all possible available data in analysis, including visual data [45]. The design of the study is limited to only text data.

4. Results and Discussion

4.1. Descriptive Data

Pilot Study

Effective research practice begins with a pilot study before the actual study is carried out ("Pilot study, the first step in research", 2017). This ensures discrepancies are traced in the proposal of the questionnaire, and though it is not required, it is encouraged ("Pilot study, the first step in research", 2017). A pilot study can be used to test data consistency and the trustworthiness of the va-

riables used in the survey questions [18]. Two IT professional took part in the pilot study test (see **Appendix C**), which included survey questions supporting the original research questions. The IT professional selected for the pilot study were well versed in cyber threat mitigation and had some degree of experience working in the financial services industry, which uses cloud computing as its primary element of infrastructure. Pilot test results did not warrant any modification to the original questions. The participants answered all questions reasonably and with clarity; there was no indication of vagueness.

4.2. Data Analysis Procedures

The study procedure was constant throughout the research and data collection. The survey process was carried out in accordance with the original interview protocol. There were no major changes, and participants incurred no financial obligations or any instabilities that could have affected the research study results. In general, the research study involved IT professionals within the United States. The target group comprised IT professionals with a lived experience in responding to cyber threats due to cloud computing. Participants were selected based on their acceptance and willingness to participate in the research study, and their experience in dealing with cyber threats due to cloud computing. According to Williams-McBean, (2019), while other research methods require a precise framework with null deviation, in qualitative research method study is based on experiences and observations that allow a researcher to follow up with additional questions [47]. The research can take advantage of this approach to curve the data to a desired saturation that increases the amount of overall information being gathered. In open-ended survey questions, participants offer accurate data regarding their experience ("Value of open-ended questions, Part 2: Implementation," 2019). Selected participants received a SurveyMonkey survey link via electronic mail (email) with an invitation letter embedded in the survey landing page (see **Appendix C**) explaining the study procedure. As survey responses were anonymous, no follow-up questions were necessary.

4.3. Demographics

The goal of the research study was to answer the research questions by exploring resilience and stability in organizations using cloud computing in their financial services. The participants came primarily from IT departments with experience in responding to cyber threats originating from the use of cloud computing as a service provider. All participants work in cyber/IT departments. Investigating the lived experiences of each participant's age group, I was able to assess cloud computing issues as they unfolded through the years. **Table 1** shows the combined years of lived experience provided by the participants.

4.4. Participants Selection and Process

Participant selection began on 13 April 2022 and ended on 12 May 2022. An invitation letter and informed consent was posted on the SurveyMonkey web page

Table 1. Demographic questions.

Code System	Participant	Gender	Age	Year of Experience	Collective of Experience	Department
MAXQDA	SP1	M	40 - 59	11 - 15	16 - 20	IT
MAXQDA	SP2	M	19 - 39	3 - 5	5 - 10	IT
MAXQDA	SP3	M	40 - 49	16 - 20	21+	IT
MAXQDA	SP4	M	19 - 39	5 - 10	5 - 10	IT
MAXQDA	SP5	M	40 - 59	11 - 15	16 - 20	IT
MAXQDA	SP6	F	40 - 59	5 - 10	16 - 20	IT
MAXQDA	SP7	F	60+	16 - 20	21+	IT
MAXQDA	SP8	M	19 - 39	5 - 10	5 - 10	IT
MAXQDA	SP9	M	40 - 49	11 - 15	16 - 20	IT
MAXQDA	SP10	F	19 - 39	5 - 10	5 - 10	IT
MAXQDA	SP11	F	40 - 49	11 - 15	21+	IT
MAXQDA	SP12	F	40 - 49	5 - 10	16 - 20	IT
MAXQDA	SP13	M	19 - 39	5 - 10	5 - 10	IT
MAXQDA	SP14	M	40 - 49	5 - 10	16 - 20	IT
MAXQDA	SP15	M	19 - 39	5 - 10	5 - 10	IT
MAXQDA	SP16	M	40 - 49	11 - 15	16 - 20	IT
MAXQDA	SP17	F	60+	16 - 20	21+	IT

on 10 April 2022 (see **Appendix C**). A link to interview questions was emailed to each candidate (see **Appendix C**). Emails were sent to over 20 IT professionals based in the United States of America (USA) using the open-source platform LinkedIn, as indicated in Research Methodology Chapter. Participants responded to 10 survey questions posted on the SurveyMonkey survey; a summary of the participants' lived experience is found in Table 1. There was no deviation in data collection, as outlined in Research Methodology Chapter. The data collection process consisted of gathering the participants' responses using the SurveyMonkey tool. Preliminary contact with targeted organizations via LinkedIn was the means by which researchers obtained participants' emails. There were no setbacks throughout the email communication process. All participants were fully informed of the research process (see **Appendix A**) consent form. The tools and data collection method outlined in Research Methodology Chapter was used. However, the MAXQDA coding tool was used to analyze data. There were no shortcomings throughout the data collection process.

4.5. Participants' Responses

The participants answered the survey questions (10 in total) as requested. Although study bias was insignificant, some participants noted that some cyber threat mitigations were more important than others. Participants' opinions

could have been drawn from his or her experience and not from the organization's bigger picture. Another bias was participants' feelings. For instance, one participant stated that the organization was not doing enough to mitigate cyber threats. This response could have been triggered by the participants' personal experience and not based on other factors. In its entirety, the data collection procedure generated a response rate of 80%, the main factor being that the responses were anonymous, and the questions were open ended. According to Ruel (2019), participants feel more at ease answering open-ended questions, which usually yield a significant response.

4.6. Data Analysis

The researchers used a reflexive thematic analysis approach to analyze the data [9]. The initial phase was open coding, which consisted in examining and reading data in order to draw a conclusion about the patterns to be coded. Gibbs (2018) stated that open coding is a means of naming, identifying, and categorizing data [45]. The researchers used Nguyen's (2016) suggestions to examine and compare data similarities and differences [18]. The researchers conceptualized the data by including a naming process that focused on participants' responses. According to Saldana (2016), in qualitative research the act of coding requires a researcher to use an analytic lens [45]. Coding was the basis for the data analysis and the development of themes, although in Research Methodology Chapter NVivo was selected as the computer-assisted qualitative data (CAQDAS) analysis; the researchers utilized the qualitative software tool MAXQDA as the CAQDAS. Qualitative Data Analysis (QDA) software provides robust functions for analyzing qualitative data. The software, which allows open-ended questions to be thematically coded [48], was used for both qualitative and mixed method according ("The architecture of MAXQDA", 2017), and using MAXQDA for qualitative data analyses helps researchers undertake a more effective analysis. MAXQDA's better features assist in classifying and quantifying parts of qualitative data. The MAXQDA software tool was able to identify weaknesses contained in the qualitative research [48]. The data collection and coding process were carried out based on the research's conceptual framework, problem statement, and research questions. The initial creation of the codes involved documenting data patterns [45]. According to Bruan and Clarker (2019b), initial coding is vital because robust raw qualitative data is collapsed into codes and data is minimized for better analysis [14]. The initial coding can help the researcher manage time [14]. Following data collection, all files containing data were simply imported into MAXQDA, which allows a researcher to upload common documents from different platforms such as pdfs, Microsoft, Excel, SurveyMonkey imports, etc. After the data import, a coding process was initiated using the MAXQDA software tool with labels for each field and data collected during the study process. The data analysis method determined the cloud computing factors that lead to cyber threats, which was the purpose of this study.

5. Study Results

5.1. Responses

The data gathered for this study was drawn from 10 survey questionnaires (see **Appendix A**). A total of 10 questionnaires were distributed to participants, all of them based on cyber threats from the use of cloud computing as a service. A summary of the survey responses was written using Braun and Clarke's (2006) thematic analysis protocol and Saldana's (2015) coding conventions [45] [46]. Additionally, the MAXQDA tool was used to classify participants' responses. Of the over 20 invitations sent out via email, 17 participants responded, one was a non-response, and two contained missing data, which meant their response was disregarded and subtracted from the original sampling. Thus, a total of two out of the total sampling received were not analyzed. The remaining 14 sampling was used to analyze and interpret data results. Data collected from the survey questionnaire was subjected to response counts, and participants' individual label. The labels were based on question frequency or occurrence; for instance, the total number of times a given response occurs. According to Guest *et al.* (2011), the use of tables comprising variables can easily quantify data that can be presented in percentage form [49].

5.2. Cloud Computing

Cloud computing services are anticipated to continue to grow as organizations seek to exploit its profits. IT decision-makers from among over 500 employees agree that cloud computing performs according to the expectations of IT professionals [5]. Additionally, cloud computing is a disruptive technology credited with providing increased speed of technology access. Organizations using cloud computing can leverage the proficiency of the advanced IT systems that would otherwise be available only to large enterprises [6]. Hence IT professionals with a knowledge of cloud computing can help minimize threats associated with its use that are found in most financial industries that utilize cloud computing to provide client services [47]. The following observations were drawn from the respondents' results of the SurveyMonkey survey questionnaire.

Question 1

Question 1 was "What threats does your organization anticipate regarding the use of cloud computing?"

To answer the question, 14 survey results from 14 IT professionals were analyzed. The data collected from each respondent was combined to form a new composite theme and map that served to refine the decision-making of the IT professional's views on the organization's threat anticipation to cloud computing. The results are shown in **Table 2**. The key components of this questionnaire are explained below. All 14 respondents described the concept and the process of anticipating cyber threats as the first defense mechanism. As shown in **Table 3**, 12 out of 14 (85%) respondents believed that insider threat was anticipated threat, while 5 out of 14 (35%) believed that SLAs were an anticipated threat.

Table 2. Responses to question 1 (N = 14).

	Theme Description	Frequency	%
Anticipated Threats	Insider threat	12	85%
	Weak service level agreement (SLA)	5	35%
	Customer data manipulation	2	14%
	Shared technology vulnerabilities	8	57%
	Abuse of cloud computing resources	10	71%
	Data segregation issues	3	21%
	Cloud security attacks	13	92%
	SLA violations	2	14%
	Data loss	14	100%

Table 3. Responses to question 2 (N = 14).

	Theme Description	Frequency	%
Detection mechanism	Positive	10	71%
	Investing in the newest technology tools	14	100%
	Use of intrusion detection tools	7	50%
	Pen testing systems on regular basis	11	78%
	Proactive monitoring to detect unauthorized activities	9	64%
	Use of external auditors		
	Negative		
	Systems developed and validated by the same team member	1	1%
	Job rotation not practised	1	1%

Based on the survey responses, 2 out of 14 (14%) respondents held similar views; 8 out of 14 (57%) believed that because of the shared technology capability, vulnerabilities were likely to be an issue when using cloud computing. Ten out of 14 (71%) respondents held similar views, with two participants stating that abuse of cloud computing resources would likely be a threat to industries. Three out of 14 (21%) stated that data separation or segregation was a weakness of cloud computing, while all 14 (100%) respondents agreed that data loss was a major threat.

Question 2

Question 2 was "What does your organization do to detect potential threats due to cloud computing?"

Table 3 above shows that at least two participants had negative views regarding how threat detection was being handled. For example, participant number10 stated that due to the shortage of IT professionals, systems were being developed and validated by the same team, which in the participant's opinion was not good

cyber hygiene. Additionally, one participant expressed concern with cyber threats stemming from the lack of job rotation practice. The remaining 12 participants expressed positive views indicating that the organizations used some type of detection mechanism. As shown in Table 4 above, 10 out of 14 respondents expressed similar views. For instance, participants three and seven stated that "new technological tools help in detecting the newest threats." All 14 respondents (100%) agreed that using intrusion detection tools was the best way to detect threats. Seven of the 14 (50%) respondents held similar views, stating that pen testing systems on a regular basis was an effective detection mechanism. Eleven out of 14 (78%) respondents believed that the proactive monitoring of authorized activities was a useful tool. Nine out of 14 (64%) respondents believed that using external auditors was beneficial to the organizations, as external auditors serve as unbiased professionals.

Question 3

Question 3 was "What does your organization do to prevent threats due to cloud computing?"

Table 4 shows participants responses grouped according to similarities. Of the 14 respondents, 10 (71%) believed that the implementation of intrusion prevention systems was an effective measure to prevent threats. One participant had a unique opinion: "Using legal contracts when providing cloud computing services." The participant indicated that drawing up legal contracts between the client and the cloud provider was necessary to implementing threat prevention. Six out of 14 (42%) study participants held similar views. For instance, three stated that limiting account access to the systems prevents potential threats. Only two participants (14%) believed that leveraging multilevel authentication was important. Thirteen out of 14 (92%) respondents expressed similar views, all of them stating that proper training contributed to threat prevention. Seven out of 14 (50%) respondents believed that implementing firewalls and security barriers was an effective prevention mechanism. Three out of 14 (21%) held similar views, stating that network access points must be secured to prevent threats. One participant had a different thought, stating that defense in depth was an essential tool of threat prevention because it comprises physical and network security.

Table 4. Responses to question 3 (N = 14).

	Theme Description	Frequency	%
Threat prevention	Implementation of IPS	10	71%
	Legal contracts	1	1%
	Account access limitation	6	42%
	Leverage multilevel authentication	2	14%
	Proper training	13	92%
	Implementation of firewall security barriers	7	50%
	Secure network access points	3	21%
	Use defense in-depth	1	1%

Question 4

Question 4 was "What does your organization do to react to cyberattacks due to its use of cloud computing?"

Table 5 shows participants' responses distributed according to similarities. Twelve out of 14 (85%) held related views. All 12 participants mentioned secure physical access as a means to react to cyberattacks. Five out of 14 (35%) believed that when cyberattacks occur, organizations should prevent additional data loss. For example, participant 10 stated that, "in the face of a cyber-attack, an organization should strengthen security systems to prevent additional data loss." Two out of 14 (14%) believed that interviews should be conducted during a cyberattack. For example, participant 9 stated, "Conducting interviews during and after a cyberattack helps in identifying the root cause." Eight out of 14 (57%) believed that conducting some type of forensics on the affected systems was an effective measure in reaction to cyberattacks. Ten out of 14 (71%) held similar opinions. For instance, participant 3 stated, "System security strengthening reacts better to cyberattacks in most cases."

Question 5

Question 5 was "What does your organization do to prevent cyberattacks due to its use of cloud computing?"

Table 6 shows data analysis results for question five. Of the 14 participants, 14 (100%) stated that employee training is the most effective means of cyberattack prevention. Eleven of the 14 (78%) held related views, with participants 9, 11, and 14 stating that "continuous security monitoring is the most effective cyberattack prevention measure. Nine out of 14 (64%) strongly supported the idea of

Table 5. Responses to question 4 (N = 14).

	Theme Description	Frequency	%
Reaction to cyberattacks	Secure physical access	12	85%
	prevent additional data loss	5	35%
	Conduct interviews	2	14%
	Conduct forensics on the affected systems	8	57%
	Systems strengthening	10	71%

Table 6. Responses to question 5 (N = 14).

	Theme Description	Frequency	%
Cyberattack prevention	Employee training	14	10%
	Continuous security monitoring	11	78%
	Implementation of IPS	9	64%
	Leverage new advancing technology	2	14%
	Maintain strong security controls	5	35%
	Comprehensive user access management to ensure the right user have access to specific information	8	57%

implementing IPS in all systems. Two out of 14 (14%) held similar views. For instance, participant 2 stated that "leveraging new and advancing technologies prepares organizations for complicated attacks." Five out of 14 (35%) indicated that maintaining strong security controls was an important component in preventing cyberattacks. Eight out of 14 (57%) held equivalent ideas. For example, participant 1 stated that "least account privilege minimizes cyberattacks," while participant 6 stated that "specific information should only be accessed by those who have the need to know."

Question 6

Question 6 was "What does your organization do to recover from cyberattacks due to its use of cloud computing?"

Table 7 shows how participants appeared to idealize their organizations when conducting cyberattack recovery. Nine out 14 (64%) participants held related opinions. For examples three of them stated that "full system backup was a good method of recovering data." Ten of the 14 (71%) indicated that leveraging cyber insurance increased recovery capability. Two out of 14 (14%) believed that replacing old technologies and systems was an effective recovery method. For example, participant 8 stated, "Investing in new technologies helped the organization enhance recovery procedures during a cyber threat." Five out of 14 (35%) stated that validation and integrity of data play an important role in the recovery process. Four out of 14 (28%) believed that the organization's written policies were effective in the recovery process. All 14 (100%) participants indicated that employee training plays an important role in cyberattack recovery. For example, participants 12 and 14 both stated that "lack of employee training can lead to attacks."

Question 7

Question 7 was "How has your organization evolved over time to enhance resilience to threats due to its use of cloud computing?"

Table 8 shows how participants responded when asked about resilience within their organization. The question received fewer responses, with only one response shared by 10 participants. One of the participants believed in using red teams in order to strengthen security. Another indicated that having a strategy

Table 7. Responses to question 6 (N = 14).

	Theme Description	Frequency	%
Resilience Enhancement	Organization's written policies were effective in the recovery process	4	28%
	Validation and integrity of data	5	35%
	Full system backup was a good method of recovering data	9	64%
	Implementing cyber security and a resilience policy framework	10	71%
	Employee training	14	100%

Table 8. Responses to question 7 (N = 14).

	Theme Description	Frequency	%
Resilience Enhancement	Utilize red teams to strengthen security systems	1	1%
	Have a strategy for verification and visibility within cyber resiliency	1	1%
	implementation of cyber security and resilience policy framework	10	71%
	Comprehensive incident management which includes threat detection	3	21%

for verification and visibility within a cyber resiliency framework for mission-essential systems is one way to enhance resilience when facing cyber threats due to the use of cloud computing. Ten out of 14 (71%) participants believed that implementing cyber security and a resilience policy framework was an effective method of enhancing resilience. Three out of 14 (21%) respondents expressed similar views. While all three mentioned incident management, participant 9 mentioned "complete incident management, which comprises threat detection and response".

Question 8

Question 8 was "How has your organization evolved over time to maintain resilience to threats due to its use of cloud computing?"

Table 9 shows that nine out of 14 (64%) participants believed that in-depth employee training can be used as a method of maintaining resilience over time. Five out of 14 (35%) respondents held similar views, two of them stating that anticipation and preparation were an effective method for organizations to maintain resilience in the face of threats. Eleven out of the 14 (78%) held similar views. For instance, one respondent stated that an "organization must create and maintain some type of business continuity cyber defense plan." All 14 participants (100%) believed that performing regular threat updates and analysis was most effective in maintaining resilience to threats. Six out of 14 (42%) held the same views. All six participants mentioned that providing clients with the right software was effective in maintaining resilience within organizations. Three of the 14 (21%) believed that implementing a better incident plan placed an organization in a better position to withstand threats.

Question 9

Question 9 was "How does your organization protect clients from data breaches?"

Table 10 below shows the results from survey questionnaire nine. Of the 14 participants surveyed, 12 (85%) believed that minimum data collection was the best way to protect client data from cyberattacks. This answer was the most widespread among the respondents. Five out of the 14 (35%) participants expressed a similar opinion. All five mentioned implementing a better data security plan as an effective method of protecting client information from cyberattacks.

Table 9. Responses to question 8 (N = 14).

	Theme Description	Frequency	%
Sustaining resilience to threats	In-depth employee training	9	64%
	Anticipation and preparation	5	35%
	Creating a better business continuity	11	78%
	Regular threat analysis update	14	100%
	Providing the right software solutions for the clients	6	42%
	Implementing a better incident response plan	3	21%

Table 10. Responses to question 9 (N = 14).

	Theme Description	Frequency	%
Protecting client data from cyber attacks	Minimum data collection	12	85%
	Implement a better data security plan	5	35%
	Use encryption for sensitive data	2	14%
	Implement least privilege and need to know in organization	8	57%
	Maintain strong SLAs	10	71%
	Develop and implement security policy to impose a set of rules for protecting client data	3	21%
	Organizations abide by CIA security model	1	1%

Two of the 14 (14%) believed that encrypting sensitive data was an effective method to protecting client data. Eight out of 14 (57%) respondents stated that practicing "least privilege and need to know" within organizations serves to protect client data. Ten out of 14 (71%) believed that an organization's implementation of strong SLAs helped protect clients from cyber threats. Three out 14 (21%) held corresponding views. For example, all three mentioned implementing some type of security, with participant 14 suggesting to "put in place security policies and impose rules that are used to protect client data." One (1%) respondent indicated that the use of the CIA model was effective in protecting client data from cyberattacks.

Question 10

Question 10 was "Is there anything you would like to add that I have not asked about?"

Question 10 was optional; the participants were given an opportunity to add any ideas they felt would benefit the study. Eleven participants had no additional input. However, participants 1, 9, and 12 each held different ideas. For example, participant 1 stated that "customer data manipulation is a threat to cloud computing as a service to financial departments." Participant 9 stated, "Cloud computing service providers do not do a good job in implementing data segregation." Participant 12 had different opinion, stating that "any shared technology possesses threat and vulnerability; thus, cloud computing in financial industries

is a nightmare." Themes produced from the data were analyzed as indicated in Tables 3-12 to include supporting statements from the respondents. Table 12 shows the predominant themes. On survey question one, all participants shared similar thoughts, stating that data loss was a common anticipated threat. For question two, all participants stated that intrusion detection was the most effective tool to implement threat-detection mechanisms. For question three, threat prevention, 92% of participants believed in effective employee training. When asked how organizations reacted to cyberattacks on question four, 85% of participants stated that physical security access was an effective security measure. On question five, all 14 (100%) participants stated that employee training was important in cyberattack prevention. For cyberattack recovery (question six), participants once again held similar views that employee training was an effective measure to implement a recovery plan. Ten respondents to question seven indicated that policy implementation and cyber security could enhance resilience, while all 14 participants on question eight held the same view, stating that regular threat analysis and software updates were efficient measures in maintaining resilience to threats. For question nine, 12 out of 14 participants stated that minimum data collection was a more effective method of protecting client data from cyberattacks. Question 10 was optional, with 57% of participants adding that shared technology was one of the issues that could cause more vulnerabilities to cloud computing as a service.

Table 11. Responses to question 10 (N = 14).

	Theme Description	Frequency	%
Participants' input	Customer data manipulation	2	14%
	Shared technology vulnerabilities	8	57%
	Data segregation	3	21%

Table 12. Emergent themes from the participants' responses (N = 14).

	Common Theme	Frequency	%
Question 1	Cloud security attacks	13	92%
Question 2	use of intrusion detection tools	14	100%
Question 3	Implementation of IPS	10	71%
Question 4	Secure physical access	12	85%
Question 5	Employee Training	14	100%
Question 6	Employee education	14	100%
Question 7	Implementation of cyber security and resilience policy framework	10	71%
Question 8	implement a better incident response plan	13	92%
Question 9	Collecting minimum data	12	85%
Question 10	Data segregation	13	92%

5.3. Summary and Observations

The purpose of collecting data from the surveyed participants was to answer the following two research questions: 1) How are organizations in the financial services industry resilient when faced with threats or losses associated with the use of cloud computing in their organization? 2) How do organizations in the financial services industry maintain stability when faced with threats or losses associated with the use of cloud computing in their organization? One of the questions often raised in qualitative survey research is whether the process used was most fitting [50]. Different factors must be examined before a suitable technique can be selected to analyze the data sets [51]. In this qualitative study, the objective of the sample size, participant responses, and the distribution of the results had to be analyzed and were the determining factors in drawing conclusions.

The data gathered from the returned survey questionnaire was subject to a precise qualitative method and analysis. The frequency distribution of each response was evaluated. The data analysis was helpful in answering the research questions. The proposed study was based on a conceptual framework comprising 14 participants. Each participant responded to nine survey questions, question 10 being optional. The participants were high-level IT professionals with experience in responding to cyber threats in a financial services industry due to cloud computing. The themes generated in the study findings suggest that the participants responded to the survey by using their lived experiences, their knowledge of the organization, and their concerns about using cloud computing in financial services.

Emergent themes. For the emergent themes, the researchers followed Nguyen's (2016) suggestion [18]. Themes with highest frequencies, for instance the number of times a response to a question was shared by the participants; then the response was termed as emergent them. Themes associated with question 1 (see **Table 2**) included insider threats, weak SLAs, client data manipulation, shared technology vulnerability, abuse of cloud computing systems, data separation issues, SLA violations, and data loss. Question two's themes (see **Table 3**) included investing in newer technological tools, using IDS tools, pen testing, proactive monitoring, and using external auditors. Themes corresponding to question 3 (see **Table 4**) included the use of defense in depth, secure network access points, implementing firewalls, proper employee training, leveraging two-factor authentication, limiting access to accounts, strengthening legal contracts, and using IPSs. Question four's related themes (see **Table 5**) included physical security access, conducting interviews, conducting forensics on affected systems, and system strengthening. Themes associated with question six (see **Table 6**) included comprehensive user access management to ensure that only the right users have access to specific information, maintaining strong security controls, leveraging new security controls, IPS implementation, continuous security monitoring, and employee training. For question seven (see **Table 7**), associated themes included employee education, using an organization's written policies, validating data in-

tegrity, replacing old technologies and old systems, leveraging cyber security insurance, and full data backups. Question eight's associated themes (see Table 8) included comprehensive incident management, cyber security, resilience policies, verifying the cyber security resilience framework, and using red teams to strengthen security. Question nine's associated themes (see Table 9) included in-depth employee training, anticipated preparation, implementing a better business continuity plan, regulatory threat updates, implementing an incident response plan, and a better software solution. Question ten's associated themes were comparable to those of questions 1 and 5; as the question was optional. The themes associated to other questions did not impact the study outcome.

6. Conclusions and Recommendations

6.1. Discussion of Findings and Conceptual Foundations

The IT professionals in this study detailed the various qualitative conceptions of cloud computing in organizations that use cloud computing in the financial industry, of which all of the ideas were included in the analysis process (see Tables 3-12). Using Nguyen's (2016) theme analysis strategy, the following primary themes were identified. For question one (see Table 3), the themes related to the interview questions were SLAs, anticipated threats, vulnerabilities, and cloud computing. For question two (see Table 4), the associated themes were the use of IDS, pen testing on a regular basis, and investing in the newest technologies. The primary themes addressed in question three (see Table 5) included implementing intrusion prevention, implementing threat prevention, limiting account access, leveraging multilevel authentication, and shared network point security.

Themes for question four (see Table 6) included physical security, if a threat has occurred, some of the participants views on preventing additional data loss, forensics on the affected systems, and systems strengthening as key themes to reacting to cyber threats. Question five's themes (see Table 7) included employee training, continuous security monitoring, IPS implementation, using new technologies, and maintaining strong security controls. Question six's themes (see Table 8) included backups, using cyber insurance system replacement, data validations, organization policies, and employee training. Question seven's themes (see Table 9) included using red teams to strengthen security systems, verification, and visibility, implementing cyber security and resilience framework, and comprehensive incident management, which includes threat detection.

Themes associated with question 8 (see Table 10) included in-depth employee training, threat anticipation and preparedness, a business continuity plan, regular threat analysis updates, using the right software, and a better incident response plan. Question nine's themes (see Table 11) included minimum data collection, implementing a data collection security plan, using encryption for sensitive data, maintaining strong SLAs, and using a CIA security model. Associated themes to question 10 (see Table 12) included customer data manipulation, vulnerability

within shared technology, and data segregation issues.

The study showed that it was possible to analyze the participants' views regarding resilience and stability in organizations using cloud computing in the financial services industry based on the research questions following the previous conceptual framework. The research used a pilot study to gain some understanding of the participants' perception. The main goal of this study was to address cyber threats faced by financial institutions that use cloud computing. The results were easily generalized, no preliminary issues were found, and the initial data analysis met all the relevant study criteria. According to Prasad, Naik, and Bapuji (2013) cloud computing provides complex advantages and benefits for organizations using its services [52]. However, the study responses show that there are several factors that weaken this robust tool. Cyber-threat issues identified by respondents were drawn from the emergent themes, which include cloud security attacks, weaknesses in IPS and IDS tools, weak physical security access, lack of employee training, weak continuity, and incident response plans.

The study attempts to address the issues and implications surrounding the use of cloud computing. In Chapter 4, attention was given to the emergent themes and emphasis was placed on the response pattern. Similar responses help redefine issues surrounding cloud computing threats. Several aspects ensuring research reliability were drawn from the emergent themes and common themes in each question. Question one's common theme was cloud security, with 13 of the 14 (92%) participants holding similar views. Question two's common theme was the use of intrusion detection based on the 14 out of 14 (100%) participants holding similar views. Question three's shared theme was IPS implementation based on the 10 (71%) participants who held similar views. Question four's common theme was secure physical access based on 12 of 14 (85%) participants. The common theme for question five was employee training, which all 14 participants shared common views, while another 100% outcome relates to question six, where education was the commonly shared view. Question seven's common theme included 71% of participants based on the views of 10 participants regarding cyberpolicies. The common theme for question eight was implementing a better incident response plan, with 13 out of 14 (92%) participants holding similar views. Question nine's common theme, based on 12 out of 14 (85%) participants, states that minimum data collection is a more effective way of avoiding threats. Although question 10 was optional, all participants responded, with data segregation being the common theme.

6.2. Implications and Connections to the Field

The services and solutions offered by cloud computing continue to grow, just as the number of organizations relying on them. Cloud computing has become prevalent in the financial services industry, with 83% of financial services institutions identifying cloud computing as a primary element of their infrastructure [29]. Although organizations rely on specific benefits of cloud computing, such

as access to critical services and lower costs, cloud computing may also create costs for organizations. The purpose of the study was to present a comprehensive review of the benefits and threats of cloud computing by investigating the resilience and stability of those organizations in the financial services industry that use cloud computing as their primary element of infrastructure. The implications of this study may benefit industries that use cloud computing as their primary source of storing client data. Financial industries, as well as other organizations using cloud computing, can utilize the data collected in this study to strengthen their cyber security defense capabilities. As data breaches due to the use of cloud computing, as indicated by respondents, are evident, organizations can benefit from this research study. The study results contain some useful findings for organizations using cloud computing to store their data. Protecting information technology systems using the means mentioned by the respondents can counter data breaches due to the use of cloud computing.

Organizations using cloud computing should understand that according to Bouwen and Stafford (2019), from 2014 to 2019 the number of cyberattacks increased by 67% and their cost by 72%, with an average cost of $13 million dollars per attack [30]. Schuh (2019) noted the importance of cyber resiliency, reflecting on the National Institute of Standards and Technology's (NIST) Special Publication 800-160 [31]. This NIST publication identified cyber resilience as involving the capacity for organizations to anticipate, withstand, recover from, and adapt to adverse conditions [31].

6.3. Recommendations

The study has several recommendations for future research. The first is geolocation. Participants might be selected from multiple countries and include a more diverse group working for IT industries. The second is that for diverse organizations, the target industries should include other industries, not only financial organizations. The third recommendation is that future scholars use multiple research methods such as a mixed or quantitative research design.

The data outcome from the participants facilitated trust in the responses from the survey questionnaire. Participant responses generated valuable information about the resilience and stability in organizations using cloud computing in the financial services industry. Furthermore, a quantitative or mixed methodology study of the resilience and stability of organizations using cloud computing in the financial services industry could help generalize the research findings.

6.4. Recommendations for Action

In order for industries to remain resilient and maintain stability while using cloud computing, technology specialists and IT professionals should be familiar with defense strategies that help reduce cyber threats. An organization's cyber security teams must implement security at the highest level. The following recommendations are suggested: 1) Proper training of all employees and system

users to encourage resilience and stability in case of cyber breaches; 2) Organizations should invest in newest cyber security technologies and 3) conduct continuous cyber security risk assessments to strengthen their systems; 4) Organizations should implement strong cyber security policies in support of cyber threat mitigation. Cyber security planning is critical to the use of cloud computing, and without proper protection there is a serious risk that cyber breaches may occur due to weak security defenses. The cyber security threat in this case is that data breaches may cause significant damage, including adding a financial burden to the organization. Hence cyber security officers should be well educated and properly informed about the cyber threats and risks associated with the use of cloud computing as a service.

The current study has provided refinements to the benefits and weaknesses associated with the use of cloud computing. The study findings provided experimental generalizability over a sample of 15 IT professionals that were asked identical questions. An effective analysis model should possess conceptual generalizability. Conceptual generalization design can be applied utilizing various methodologies across a larger pool of IT professionals to provide similar study results. To determine the conceptional generalizability of resilience and stability in organizations using cloud computing in the financial services industry, further research is needed. The findings from the study results offer a basis for future research studies to investigate cyber threats due to the use of cloud computing. The following steps, if applied, might help researchers obtain positive results: 1) employ participants from multiple locations, 2) include mixed methodologies to obtain different results, and 3) involve different organizations to obtain diverse outcomes.

6.5. Implications for Technological Change

The current study contains implications for technological change. The literature review indicated that cloud computing is a disruptive technology that organizations across several industries rely on as a tool to support greater technological capacity and access to a diverse network of digital tools. Cloud computing is an information system networking strategy that involves an organization relying on larger, centralized information systems that offer greater data storage or information system power [23]. If the connection developed between security and the defense mechanism is successful, organizations will be able to utilize cloud computing and have fewer data breaches, resulting in a more resilient and stable industry overall.

Cyber security is a critical part of cloud computing as a service, and this research study has crucial implications for organizations that use cloud computing as a service. The study proposes strategies that can improve cyber security and its defense capabilities. It adds value to the cyber security field by exploring the security threat factors as well as organizational resilience and stability. The research expands our understanding of not only security weaknesses but also of

the benefits associated with the use of cloud computing.

6.6. Implications for Practice

The growth of cloud computing is expected to continue as organizations seek to exploit its benefits. However, there are challenges in using and deploying cloud computing. These challenges include cost, governance, and security, among others. Organizations face continuous challenges when utilizing cloud computing, and so it can be difficult to completely eliminate cyber threats. However, organizations must also be able to implement strategies that mitigate cyber threats and leverage technologies, IT professionals, and appropriate resources in order to combat threats due to the use of cloud computing. This study's research results are a major step in understanding the threats associated with the use of cloud computing and the possible defense mechanisms to be deployed. Cyber security officers tasked with defending systems must understand their weaknesses and defense mechanisms. Furthermore, all employees, as they are the first line of defense, should be trained to ensure greater defense effectiveness. Organizations need to understand the cause and effects of using cloud computing; the study results shows that a lack of training and the absence of IPS or IDS can lead to security breaches. Organizations that use cloud computing often rely on systems such as IPS, IDS, and policies to detect and mitigate cyber threats. The study findings indicate that organizations should invest in newer technologies and acquire the very latest security software.

6.7. Conclusions

The purpose of this study was to explore the resilience and stability of subject matter experts who use cloud computing in the financial services industry. A qualitative, descriptive research methodology and design were used to explore the research problem. The target population of this study was IT professionals working in the financial services industry. The experience of 15 IT professionals was surveyed to analyze cyber threats associated with cloud computing. Interview data was used to answer two research questions: How do organizations in the financial services industry remain resilient when faced with threats or losses associated with their use of cloud computing? How do organizations in the financial services industry maintain stability when faced with threats or losses associated with their use of cloud computing? A comparison of the survey outcome and the literature contained in the study shows that organizations can use available resources to tighten cyber security threats and become more resilient when faced with threats due to the use of cloud computing. The current literature stresses the benefits of using cloud computing and suggests ways to secure systems. Industries that invest in better security systems have a better chance of mitigating cyber threats due to the use of cloud computing, as well as of reducing the costs associated with security breaches. The study findings indicate that although systems updates and security defense are important, employee training plays a paramount role in mitigating security breaches.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Accenture (2020) Cloud Outcomes Survey: Expectation vs. Reality. Accenture. https://www.accenture.com/us-en/insights/cloud/cloud-outcomes-perspective

[2] Rosati, P., Fox, G., Kenny, D. and Lynn, T. (2017) Quantifying the Financial Value of Cloud Investments: A Systematic Literature Review. 2017 *IEEE International Conference on Cloud Computing Technology and Science* (*CloudCom*), Hong Kong, 11-14 December 2017, 194-201. https://doi.org/10.1109/CloudCom.2017.28

[3] Maufe, Z. (2020) Financial Services, Cloud Adoption, Regulators. Google Cloud Blog. https://cloud.google.com/blog/topics/inside-google-cloud/new-study-shows-cloud-adoption-increasing-in-financial-services

[4] Sampson, D. and Chowdhury, M.M. (2021) The Growing Security Concerns of Cloud Computing. 2021 *IEEE International Conference on Electro Information Technology* (*EIT*), Mt. Pleasant, 14-15 May 2021, 50-55. https://doi.org/10.1109/EIT51626.2021.9491902

[5] Woods-Moss, J. (2015) Cloud Hype Not Hyped Enough. TATA Communications. https://www.tatacommunications.com/blog/2015/02/cloud-hype-not-hyped-enough

[6] Jackson, K.L. and Goessling, S. (2018) Architecting Cloud Computing Solutions: Build Cloud Strategies That Align Technology and Economics While Effectively Managing Risk. Packt Publishing, Birmingham.

[7] Mallette, M.H. and Duke, N.K. (2020) Literacy Research Methodologies. 3rd Edition, Guilford Publications, New York.

[8] Deloitte (2021) Cloud Banking: More than Just a CIO Conversation. Deloitte. https://www2.deloitte.com/global/en/pages/financial-services/articles/bank-2030-financial-services-cloud.html

[9] Mlitz, K. (2021) Enterprise Cloud Computing Challenges 2019-2020. Statista. https://www.statista.com/statistics/511283/worldwide-survey-cloud-computing-risks

[10] Qi, Y. and Xiao, J. (2018) Fintech: AI Powers Financial Services to Improve People's Lives. *Communications of the ACM*, **61**, 65-69. https://doi.org/10.1145/3239550

[11] Neubauer, B.E., Witkop, C.T. and Varpio, L. (2019) How Phenomenology Can Help Us Learn from the Experiences of Others. *Perspectives on Medical Education*, **8**, 90-97. https://doi.org/10.1007/S40037-019-0509-2

[12] Adams, W. (2015) Conducting a Structured Questionnaire.

[13] Clarke, V. and Braun, V. (2014) Thematic Analysis. In: Teo, T., Ed., *Encyclopedia of Critical Psychology*, Springer, Berlin, 1947-1952. https://doi.org/10.1007/978-1-4614-5583-7_311

[14] Braun, V. and Clarke, V. (2019b) Reflecting on Reflexive Thematic Analysis. *Qualitative Research in Sport, Exercise and Health*, **11**, 589-597. https://doi.org/10.1080/2159676X.2019.1628806

[15] Nayyar, A. (2019) Handbook of Cloud Computing: Basic to Advanced Research on the Concepts and Design of Cloud Computing. BPB Publications, Noida.

[16] Lee, I. (2021) Cybersecurity: Risk Management Framework and Investment Cost

Analysis. *Business Horizons*, **64**, 659-671.
https://doi.org/10.1016/j.bushor.2021.02.022

[17] Mester, L.J. (2019) Cybersecurity and Financial Stability. Federal Reserve Bank.

[18] Nguyen, D.S. (2016) Workplace Factors That Shape IT Project Success. *International Journal of Computer* (*IJC*), **20**, 83-156.
https://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/538

[19] Scott, W.R. (1995) Institutions and Organizations. Sage, Thousand Oaks.

[20] Scott, R.W. (2004) Institutional Theory. In: Ritzer, G., Ed., *Encyclopedia of Social Theory*, Sage, Thousand Oaks.

[21] Xiao, L. and Cao, H. (2017) Organizational Resilience: The Theoretical Model and Research Implication. *ITM Web of Conferences*, **12**, Article No. 04021.
https://doi.org/10.1051/itmconf/20171204021

[22] Fusch, P.I. and Ness, L.R. (2015) Are We There Yet? Data Saturation in Qualitative Research. *The Qualitative Report*, **20**, 1408-1416.
https://doi.org/10.46743/2160-3715/2015.2281

[23] Ransome, J.F. (2017) Cloud Computing: Implementation, Management, and Security. CRC Press, Boca Raton.

[24] Lengnick-Hall, C.A., Beck, T.E. and Lengnick-Hall, M.L. (2011) Developing a Capacity for Organizational Resilience through Strategic Human Resource Management. *Human Resource Management Review*, **21**, 243-255.
https://doi.org/10.1016/j.hrmr.2010.07.001

[25] Meyer, J.W. and Rowan, B. (1977) Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology*, **83**, 340-363.
https://doi.org/10.1086/226550

[26] Duchek, S. (2020) Organizational Resilience: A Capability-Based Conceptualization. *Business Research*, **13**, 215-246. https://doi.org/10.1007/s40685-019-0085-7

[27] Barley, S.R. and Tolbert, P.S. (1997) Institutionalization and Structuration: Studying the Links between Action and Institution. *Organization Studies*, **18**, 93-117.
https://doi.org/10.1177/017084069701800106

[28] Lamba, A. (2018) Protecting the "Cybersecurity & Resiliency" of the Nation's Critical Infrastructure: Energy, Oil & Gas. *International Journal of Current Research*, **10**, 76865-76876. https://doi.org/10.2139/ssrn.3535434

[29] Annarelli, A. and Nonino, F. (2016) Strategic and Operational Management of Organizational Resilience: Current State of Research and Future Directions. *Omega*, **62**, 1-18. https://doi.org/10.1016/j.omega.2015.08.004

[30] Bouwens, C.L. and Stafford, R.B. (2019) The Role of Organizational Resilience across the Cyber Attack Lifecycle. In: *Proceedings of the International Annual Conference of the American Society for Engineering Management*, American Society for Engineering Management (ASEM), Huntsville, 1-8.

[31] Schuh, D.L. (2020) The Cyberspace Advantage: Inviting Them In-How Cyber Deception Enables Better Resilience. MITRE Corp.

[32] Anderson, T., Busby, J., Gouglidis, A., Hough, K., Hutchison, D. and Rouncefield, M. (2020) Human and Organizational Issues for Resilient Communications. In: Rak, J. and Hutchison, D., Eds., *Guide to Disaster-Resilient Communication Networks*, Springer, Cham, 791-807. https://doi.org/10.1007/978-3-030-44685-7_32

[33] Galinec, D. and Luić, L. (2019) Digital Security Perspectives and Engagement for Resilience in Information-Communication Environment. 2019 3*rd European Conference on Electrical Engineering and Computer Science* (*EECS*), Athens, 28-30

December 2019, 106-112. https://doi.org/10.1109/EECS49779.2019.00032

[34] Thorisson, H., Baiardi, F., Angeler, D.G., Taveter, K., Vasheasta, A., Rowe, P.D. and Linkov, I. (2019) Resilience and Hybrid Threats: Security and Integrity for the Digital World. IOS Press, Amsterdam.

[35] Guetterman, T.C. (2020) Qualitative, Quantitative, and Mixed Methods Research Sampling Strategies. Education. https://doi.org/10.1093/obo/9780199756810-0241

[36] O'Hanlon, F. (2018) Mixed-Methods Research: Achieving a Robust Design. In: *Building Research Design in Education*: *Theoretically Informed Advanced Methods*, Bloomsbury Academic, London, 107-130. https://doi.org/10.5040/9781350019539.ch-007

[37] Heale, R. and Twycross, A. (2017) What Is a Case Study? *Evidence Based Nursing*, **21**, 7-8. https://doi.org/10.1136/eb-2017-102845

[38] Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N. and Aboagye-Sarfo, P. (2018) Application of Four-Dimension Criteria to Assess Rigour of Qualitative Research in Emergency Medicine. *BMC Health Services Research*, **18**, Article No. 120. https://doi.org/10.1186/s12913-018-2915-2

[39] Cutcliffe, J.R. and McKenna, H.P. (1999) Establishing the Credibility of Qualitative Research Findings: The Plot Thickens. *Journal of Advanced Nursing*, **30**, 374-380. https://doi.org/10.1046/j.1365-2648.1999.01090.x

[40] Birt, L., Scott, S., Cavers, D., Campbell, C. and Walter, F. (2016) Member Checking: A Tool to Enhance Trustworthiness or Merely a Nod to Validation? *Qualitative Health Research*, **26**, 1802-1811. https://doi.org/10.1177/1049732316654870

[41] Connelly, L.M. (2016) Trustworthiness in Qualitative Research. *MEDSURG Nursing*, **25**, 435-436.

[42] Shenton, A.K. (2004) Strategies for Ensuring Trustworthiness in Qualitative Research Projects. *Education for Information*, **22**, 63-75. https://doi.org/10.3233/EFI-2004-22201

[43] Braun, V. and Clarke, V. (2019) Thematic Analysis. In: Liamputtong, P., Ed., *Handbook of Research Methods in Health Social Sciences*, Springer, Berlin, 843-860. https://doi.org/10.1007/978-981-10-5251-4_103

[44] Braun, V. and Clarke, V. (2013) Successful Qualitative Research: A Practical Guide for Beginners. Sage, Thousand Oaks.

[45] Saldana, J. (2015) The Coding Manual for Qualitative Researchers. Sage, Newcastle upon Tyne.

[46] Braun, V. and Clarke, V. (2006) Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, **3**, 77-101. https://doi.org/10.1191/1478088706qp063oa

[47] Williams-McBean, C.T. (2019) The Qualitative Report. *Fort Lauderdale*, **24**, 1055-1064.

[48] Silver, C. and Lewin, A. (2014) Using Software in Qualitative Research: A Step-by-Step Guide. Sage Publications Ltd., Thousand Oaks. https://doi.org/10.4135/9781473906907

[49] Guest, G., MacQueen, K.M. and Namey, E.E. (2011) Applied Thematic Analysis. Sage Publications, Thousand Oaks. https://doi.org/10.4135/9781483384436

[50] Billups, F.D. (2019) Qualitative Data Collection Tools: Design, Development, and Applications (Qualitative Research Methods).

[51] Adu, P. (2019) A Step-by-Step Guide to Qualitative Data Coding. Routledge, London. https://doi.org/10.4324/9781351044516

[52] Prasad, M.R., Naik, R.L. and Bapuji, V. (2013) Cloud Computing: Research Issues and Implications. *International Journal of Cloud Computing and Services Science*, **2**, 134-140. https://doi.org/10.11591/closer.v2i2.1963

Appendix A: Informed Consent Form

Aspen University
School of Education
1660 S. Albion St., Suite 525
Denver, CO 80222
Email: irb@aspen.edu

Title of Study

Resilience and Stability in Organizations Using Cloud Computing in the Financial Services Industry

Introduction:

The purposes of this form are to provide you (as a prospective research study participant) information that may affect your decision as to whether to participate in this research and to record the consent of those who agree to be involved in the study.

Research:

Juliette Sondano has invited your participation in a research study. I am completing this research as part of my doctoral degree.

Purpose of Study:

The purpose of the research is to explore the resilience and stability of subject matter experts using loud computing in the financial services industry. The proposed dissertation explored how organizations are resilient and maintain stability when faced with threats or losses associated with the use of cloud computing in their organization

Participant Eligibility Survey:

You are eligible to participate in this research if you:

a) Currently work for a financial services organization in the United States

b) Worked for this organization for the last three years or longer

c) Your current position include tasks and duties are related to cybersecurity

d) You are 18 years of age or older

Description of the Research Activity:

If you decide to participate, then as a study participant you will be asked to:

a) To respond to an online survey question using SurveyMonkey Survey

b) LinkedIn audio recording

Approximately (15) of subjects will be participating in this research study.

Risks:

If you decide to participate in this research study some risks may include:

a) Confidentiality

To decrease the impact of these risks, you can:

a) Stop participation at anytime

b) Choose not to respond to the survey

c) Survey responses will be anonymized. Once the data is collected all participants identifiable personnel information was disassociated from the data. The results identify each respondent as subject 1, subject 2 etc.

Benefits:

Benefits of participating in this study include:

Be a part of the few that are trying to find solution for the future computing threat mitigation

Confidentiality:

All information obtained in this study is strictly confidential unless disclosure is required by law. The results of this research study may be used in reports, presentations, and publications, but the researchers will not identify you. In order to maintain confidentiality of your records, name of personal identifiable information (PII) will be protected, and any survey results were anonymized. The people who will have access to your information are myself, and/or, my dissertation committee. I will secure your information with these steps: securing the computer containing your file information in a protected area. Data transfer was encrypted. I will delete electronic data and destroy paper data after 3 years. The stored data had no PII associated to it as all PII was redacted during data analysis phase.

Withdrawal Privileges:

It is okay for you to decline to participate in this research study. You are free to stop participating at any time and there will be no penalty to you. If you decide to stop participation, you may do so by emailing me at julieshaidi3@gmail.com or calling/text at 573-382-8147. Your decision will not affect your relationship with Aspen University or otherwise cause a loss of benefits to which you might otherwise be entitled.

Costs and Payments:

There is no financial cost to you as a participant in this study, nor is there payment for your participation.

Voluntary Consent:

Any questions you have concerning the research study or your participation in the study will be answered by Dr. Dan, Nguyen at, dan.nguyen@aspen.edu. If you have questions about your rights as a subject/participant in this research, or if you feel you have been placed at risk, you can contact the Institutional Review Board at IRB@Aspen.edu. This form explains the nature, demands, benefits and any risk of the research study. By clicking "I Agree" you confirm that you are 18 years or older, understand the content of this form, and agree to participate in this study.

----I Agree ---- I Do Not Agree

Appendix B: Recruitment Announcement

Participant Recruitment Announcement/Invitation Letter

Greetings, my name is Juliette Sondano. I am a doctoral student at the Aspen University. I am conducting research on Resilience and Stability in Organizations Using Cloud Computing in the Financial Services Industry, and I am extending an invitation to you due to you work in an organization that uses cloud computing to support its customers.

Participation in this research consist of an online survey about your experience in handling a breach or loss due to cloud computing issues which will take approximately 10 minutes.

If you have any concerns or questions or would like to be part of this research, please contact me at 573-382-8147 or julieshaidi90@gmail.com.

Appendix C: Participant Eligibility Survey

1) Do you currently work for a financial services organization in the United States?

2) Have you worked for this organization for the last three years or longer?

3) Does your current position include tasks and duties that are related to cybersecurity?

4) Are you 18 years or older in age?

Structured questionnaire Protocol

Survey Questions

1) What threats does your organization anticipate regarding the use of Cloud computing? Which of these threats are most likely? Please explain in one to three sentences

2) What does your organization do to detect threats due to Cloud computing? What technologies are in place? Please explain in one to three sentences

3) What does your organization do to prevent potential threats due to Cloud computing? Please explain in one to three sentences

4) What does your organization do to react to cyberattacks due to its use of Cloud computing? Please explain in one to three sentences

5) What does your organization do to prevent to cyberattacks due to its use of Cloud computing? Please explain in one to three sentences

6) What does your organization do to recover from cyberattacks due to its use of Cloud computing? Please explain in one to three sentences

7) How are organizations in the financial services industry resilient when faced with threats? Or losses associated with the use of cloud computing in their organization.

8) How do organizations in the financial services industry maintain stability or sustain resilience when faced with threats or losses associated with the use of cloud computing in their organization?

9) What does your organization do to Protecting client's data from cyberattacks? cyberattacks due to its use of Cloud computing? Please explain in one to three sentences

10) Is there anything you would like to add that I have not asked about? Please explain in one to three sentences

Demographic questionnaire

What is your gender? (Please check one)

☐ M ☐ F

What is your age (Please check one)

☐ 19 - 39 ☐ 40 - 59 ☐60+

How many years of experience do you have responding to cyber threats as a result of cloud computing in financial industry? (Please check one)

☐ 3 - 5 ☐ 5 - 10 ☐ 11 - 15 ☐ 16 - 20 ☐ 21+

Appendix D: IRB Review Form DDCS

IRB Review Form DSCS

IRB Case Number: 5JS2-22F2

Name of Candidate: Juliette Sondano

Title: Resilience and Stability in Organizations Using Cloud Computing in the Financial Services Industry

Approval Expires on: 2/24/23

Application Type:

_X_Exempt Review

__Expedited Review

__Full Review

Application Status:

_X_Approved

___Not Approved

___Approved with Amendment

The student/researcher understands and agrees to maintain the confidentiality of any entity agreeing to assist with providing data; to obtain informed consent from any human participants in the study; and to retain and safeguard written

consents and the data for a period of five years from all entities, presenting copies to Aspen University, to the participants, and to authoritative bodies when appropriate.

2/24/2022

Heather Frederick, IRB Chair

All questions or concerns should be directed to IRB@aspen.edu. This includes immediately reporting any unexpected adverse events or alterations in risk levels for participants within 48 hours of occurrence of such events.

Aspen University
1660 South Albion Street, Suite 525
Denver, CO 80222