

1-29-2026

Better IT Disaster Recovery and Procedures to Improve Response after Computer Crime

Allan Eduardo Arroyo-Melendez
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management & Human Potential

This is to certify that the doctoral study by

Allan E. Arroyo-Melendez

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee

Dr. Dana Haywood, Committee Chairperson, Information Technology Faculty

Dr. Geraldine Light, Committee Member, Information Technology Faculty

Chief Academic Officer and Provost

Sue Subocz, Ph.D.

Walden University

2026

Abstract

Better IT Disaster Recovery and Procedures to Improve Response after Computer Crime

by

Allan E. Arroyo-Melendez

MS, Grantham University, 2019

BS, Grantham University, 2016

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

March 2026

Abstract

A lack of an effective disaster recovery plan (DRP) can negatively impact business outcomes following a cyberattack. Information technology (IT) managers are concerned that the lack of DRP may increase the risk of ransomware, fines, and public distrust. Grounded in the unified theory of acceptance and use of technology, the purpose of this qualitative pragmatic inquiry study is to explore strategies that some IT managers use to implement a DRP. The participants are four IT managers in the southeast United States. Data were collected through semistructured interviews and a review of publicly available documents. Through thematic analysis, three themes were identified: (a) implementation during attack, (b) continuous training, and (c) implementation constraints. The key recommendations are that organization should include DRP into their cybersecurity strategy to allow recovery and continuing operations after a cyberattack. The implication for positive social change is that these strategies may enable the continuation of critical services in facilities such as hospitals, helping to prevent life-threatening situations during a disaster.

Better IT Disaster Recovery and Procedures to Improve Response after Computer Crime

by

Allan E. Arroyo-Melendez

MS, Grantham University, 2019

BS, Grantham University, 2016

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

March 2026

Dedication

I dedicate this study to my Mother, who taught me to finish everything I start and to educate my mind. To my brother, sister, nephews, and nieces, for serving as inspiration to progress.

Acknowledgments

First, I want to thank God for staying with me and helping me continue when I wanted to stop. To my family, for their support and motivation, which has always encouraged me to continue my education. Special thanks to Sandra, who always supported and encouraged me to finish. Lastly, I want to thank my committee members, Dr. Haywood and Dr. Light. Also, thank you to all the ex-alumni of Colegio La Merced de Puerto Rico!

Table of Contents

List of Tables	iv
Section 1: Foundation of the Study.....	1
Background of the Problem	1
Information Technology Problem Focus and Project Purpose	2
Research Question(s)	2
Assumptions and Limitations	2
Assumptions.....	2
Limitations	3
Significance of the Study	3
Contribution to Information Technology Practice.....	3
Implications for Social Change.....	3
Transition and Summary.....	4
Section 2: Literature Review	5
A Review of the Professional and Academic Literature.....	5
Conceptual Framework.....	6
Disaster Recovery	9
Disaster Recovery Plan Challenges	14
Business Continuation	15
BCP and DRP in the Cloud.....	16
Resilience.....	20
Using the Framework with the Topic	25

Transition and Summary	27
Section 3: The Project.....	28
Project Ethics	28
Nature of the Study	31
Research Method	32
Research Design.....	32
Population, Sampling, and Participants	34
Data Collection Activities.....	36
Interview Questions	38
Data Organization and Analysis Techniques	39
Study Validity	41
Reliability.....	41
Validity	42
Transition and Summary.....	45
Section 4: Application to Professional Practice and Implications for Change	46
Presentation of the Findings.....	47
Implementation During Attack	47
Continuous Training	51
Implementation Constraints	53
Information Technology Contributions and Recommendations for	
Professional Practice	57
Implications for Social Change.....	58

Recommendations for Further Research.....	60
Conclusions.....	62
References.....	63
Appendix A: CITI Certifications	91
Appendix B: Interview Protocol.....	92

List of Tables

Table 1 *Summary of Themes* 46

Section 1: Foundation of the Study

Background of the Problem

There is a need for comprehensive disaster recovery and continuity implementation programs for organizations to protect their information systems (IS) and information technology (IT). Kesa (2023) stated that implementing Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) programs faced challenges such as evolving technologies, system complexity, budget constraints, and frequent organizational resistance. While international standards guided the implementation of business continuity management (BCM), Russo et al. (2023) noted a gap in communicating metrics for program assessment and understanding complex relationships in disaster management. Obtaining a practical implementation required a comprehensive understanding of IT infrastructure, risk assessment, and robust recovery strategies (Pinto et al., 2022). Meanwhile, Meechang and Watanabe (2022) highlighted that DRP and BCP added top management support, information sharing, and government involvement as necessary components. Moreover, cloud computing provided a readily available, geographically dispersed infrastructure for data backup and disaster recovery, allowing businesses to continue operations even during disruptions. However, potential issues, such as reliance on internet connectivity and vendor lock-in, needed to be carefully considered and addressed within the DRP and BCP strategy (Kesa, 2023). Understanding how these challenges affected the adoption of DRP and BCP could have helped form strategies for implementation.

Information Technology Problem Focus and Project Purpose

The specific IT problem was that some IT managers in business organizations lacked effective strategies for implementing DRP. The purpose of this qualitative pragmatic inquiry study was to explore strategies that some IT managers used to implement a DRP in the Southeast United States. The IT managers need at least 10 years of experience in cloud computing technology and implementing DRP and BCP. I selected four managers using purposive sampling to conduct semi-structured interviews. Additionally, I collected publicly available documents on the subject matter to triangulate the participants' interviews. I grounded this study on Venkatesh et al.'s unified theory of acceptance and use of technology (UTAUT) from 2003. The theory utilizes constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions to examine the intention to adopt (behavioral intention) and actual adoption (use behavior). I used these constructs, which measured specific perceptions, to analyze how perceived job performance, ease of use, social engagement, and support systems affected an organization's users in adopting DRP and BCP policies implemented by IT managers.

Research Question(s)

What strategies do some IT managers use to implement disaster recovery plans?

Assumptions and Limitations

Assumptions

An assumption is a statement accepted as true without supporting evidence (Li & Li, 2024). I assumed that each participant would answer each interview question wholly

and honestly. I also assumed I would find ample participants in the Southeast region of the United States.

Limitations

A limitation is a weakness in a research design that might have created a challenge with the results (Dewey, 2024). The limitations were time usage and the availability of participants. I planned tasks carefully to minimize the time necessary to complete them. I searched social media sites, such as LinkedIn, to find participants and alleviate access issues.

Significance of the Study

Contribution to Information Technology Practice

This study provides fresh implementation strategies for IT managers in any company implementing a DRP and BCP to prevent a complete shutdown after a cyberattack. The strategies addressed barriers to adopting these plans and how to overcome them. Barriers, such as the implementation of DRP and BCP, hindering employee performance, were considered to prevent a lack of adoption, which would have impeded the response to the next cyber-attack. The improved acceptance of DRP and BCP implementation may have decreased the gap between cyberattacks and recovery, while protecting critical data, such as personally identifiable information (PII).

Implications for Social Change

DRP and BCP are crucial for organizations to maintain operations and protect sensitive information during disruptions (Bocchi et al., 2024; Kesa, 2023). DRP and BCP may be critical for social change and society because they enable organizations and

communities to maintain essential functions and services (Bocchi et al., 2024; Kesa, 2023). DRP and BCP provided peace of mind to society during and after disruptive events, such as natural disasters, cyber-attacks, and the recent pandemics, by minimizing the impact on people's lives, promoting societal resilience and stability, and facilitating a quicker recovery process for regular life continuity (Sasaki et al., 2020). DRP and BCP can contribute to social change by maintaining critical services, promoting economic stability, reducing vulnerability, enhancing community resilience, and fostering social cohesion (Plaka, 2022).

Transition and Summary

Section I introduces the problem of understanding the factors that affect the success of DRP and BCP after a cyber-attack. In this section, I discuss the background of the problem, the information technology issue, and the project's purpose. Moreover, I included the research question and provided a detailed explanation of the study's significance, including its contribution to information technology practice, assumptions, and limitations. Finally, I described the significance of the study and concluded with a declaration of positive social change. I included a literature review in Section 2 to cover methodologies, the definitions of DRP and BCP, and a detailed definition of UTAUT. Furthermore, I presented my research design in Section 3 and analyzed the data collected in Section 4.

Section 2: Literature Review

A Review of the Professional and Academic Literature

My focus is on providing a comprehensive review of the existing knowledge and opinions related to the research question of my study: What strategies can some IT managers implement for a DRP? I will explore the conceptual framework of UTAUT by analyzing and identifying critical measures that trigger the IT manager's implementation decision. I have selected over 200 articles, of which 85 % were peer-reviewed within 5 years of any anticipated graduation date. I selected the following databases: IEEE Xplore Digital Library articles, Academic OneFile, Biography (Gale in Context), Directory of Open Access Journals, Educator's Reference Complete, and more. I used the following key phrases for the search: *strategies to implement disaster recovery and continuity, using innovative technologies for disaster recovery and continuity implementation, combining innovative technologies such as cloud computing for disaster recovery and continuity, difficulties in disaster recovery and continuity management of disaster recovery and continuity after implementation, disaster recovery and continuity history, disaster recovery, and continuity importance.*

First, I will discuss the UTAUT as a conceptual framework and its uses, and compare it to similar acceptance theories. I will then discuss DRPs and the challenges of implementing them into modern IT infrastructure. I will continue to discuss BCP within organizations and how it affects them. I will tie it together with how cloud computing can implement DRP and BCP while also exploring infrastructure resilience. Finally, I will tie

DRP and BCP into the UTAUT framework to help explain how I will analyze interviews for themes.

Conceptual Framework

Using the UTAUT, I will explain why some IT managers resist using technology to their advantage, and suggest additional strategies for implementing disaster recovery work. The benefit of the UTAUT model is that it employs several constructs, including performance expectancy, effort expectancy, social influence, facilitating conditions, and moderator constructs (Venkatesh et al., 2003). These concepts check factors related to people's intention to adopt (behavioral intention) and actual adoption (use behavior). Therefore, some might adopt or not adopt it, and the theory will help analyze both approaches.

Several theoretical models have been developed for more than four decades to understand the acceptance and use of IS and IT. Moreover, several research studies have been conducted on technology adoption by groups and organizations trying to prove that one must first use technology before achieving desired outcomes, such as job performance and employee productivity (Venkatesh et al., 2003). Many researchers explore approaches to explain and predict user behavior and acceptance in IT. These theories include diffusion of innovations (DOI) by Rogers (1995), the theory of reasoned action (TRA) by Fishbein and Ajzen (1975), the theory of planned behavior (TPB) by Ajzen (1991), the decomposed theory of planned behavior by Taylor and Todd (1995), and technology acceptance model TAM by Davis (1989). Venkatesh et al. (2003)

synthesized seven competing models into the UTAUT to capture more explanatory power than the individual theories did individually.

Characteristic of UTAUT

The theory can be used to examine factors related to people's intention to adopt and actual adoption (Venkatesh et al., 2003). The six constructs that explore acceptance are performance expectancy, effort expectancy, social influence, facilitating conditions, behavior intention, and use behavior. Furthermore, the theory explains the influence of the constructs with the moderators of age, gender, experience, and voluntariness (Venkatesh et al., 2003). Researchers use these constructs to examine users' behaviors when adopting technology, while the moderators provide insight into why they lean toward a particular direction of acceptance.

Performance expectancy focuses on how users perceive modern technology to improve their job performance (Venkatesh et al., 2003). This construct played a significant role in understanding how users perceived their performance in technology, such as e-procurement and language learning (Shatta, 2021; Wang & Xue, 2022). Do et al. (2023) stated that setting appropriate expectations for conversational agents, facilitating group discussions, and positively influencing the performance expectancy impact on adoption. Ayaz and Yanartas (2020) confirmed that this construct operates in multiple situations, varying in terms of voluntariness and experience levels.

Effort expectancy focuses on how users perceive the ease of use of technology (Venkatesh et al., 2003). Alabdullah et al. (2020) employed this construct to examine how ease of use influences dental students' acceptance of tele-dentistry instruments. They

found that introducing tele-dentistry in schools reduced ease-of-use barriers and may improve overall adoption among students entering the field. Similar findings were discovered in a study on using electric vehicles in Indonesia (Gunawan et al., 2022) and IoT in Taiwan's construction industry (Chen et al., 2020).

Social influence focuses on how users perceive that others' attitude toward a technology affects their decision to adopt it (Venkatesh et al., 2003). This influence can occur through leadership, norm formation, and mass mediation (Sammut & Bauer, 2020). For example, teachers may influence students in a mentoring role, which can influence the students to adopt technology or lessons (Butera et al., 2020). The conclusion is that a positive social influence may lead to higher intent to adopt.

Facilitating conditions focus on users' perceptions that they have the necessary support to use a particular technology. Jerez et al. (2021) noted that these conditions encompass technological support, resource availability, and organizational backing. These items impacted students' and teachers' attitudes toward learning management systems in rural areas of China during the COVID-19 pandemic. Without those using the technology believing that support for the technology existed, it would have negatively influenced their acceptance, despite it being a necessity during the health crisis (Wang, 2021).

Behavioral intention focuses on the user's desire to adopt technology, while user behavior leans toward the actual adoption (Venkatesh et al., 2003). These constructs have been used to measure how the previous constructs influenced the adoption of technology such as chatbots, place attachment, and cryptocurrency (Bhuvana & Aithal, 2022; Dang

& Weiss, 2021; Gatzoufa & Saprikis, 2022). As noted in public media, these items have received acceptance amongst the public, and developers accounted for the distinct factors that would help or hinder their ability to deploy their technology successfully.

Usability of UTAUT

A key attribute of the UTAUT model is its applicability to any situation. It has been utilized to examine the adoption of various technologies in different areas, including mobile health, electronic government, mobile banking, mobile payments, m-wallets, smartphones, mobile commerce, and blockchain (Dwivedi et al., 2020). For example, Chroustová et al. (2022) used it to determine chemistry teachers' acceptance of educational software in secondary education. Shaya et al. (2023) found it helpful in determining influencing factors toward adopting mobile learning platforms. Dewi et al. (2023) employed UTAUT to investigate ICT adoption during the COVID-19 pandemic, encompassing education, healthcare, and mobile technology. Finally, Tamilmani et al. (2021) noted that it has been cited in more than 6,000 publications in information systems and beyond. The UTAUT model has been applied to study the adoption of remote healthcare technology, e-banking, smartphones, and mobile applications (Ahmed et al., 2023; Kamal & Subriadi, 2021; Malik, 2020; Rouidi et al., 2022).

Disaster Recovery

DRP is an ongoing process that requires regular review, updates, and maintenance because risks, technology, and government-business requirements change periodically. Therefore, the DRP lifecycle should be followed, including risk assessment, business impact analysis (BIA), policy creation, awareness training, documentation and data

backup, resource planning, testing and maintenance procedures, and review of audit results (Shetty et al., 2022). These checkpoints provide a robust method for handling disaster recovery.

Ganesen et al. (2022) emphasized the importance of IT risk assessment by examining how the rapid advancement of cybercriminals affects organizations that rely on IT infrastructure. IT managers have been forced to continually update their risk and security processes to address the challenges presented by hackers. Ganesan concluded that risk assessment and management should follow solutions that implement technological and educational approaches.

The first step would be to establish a risk assessment. Alshahrani et al. (2019) defined risk assessment as a process that involves identifying, prioritizing, and mitigating potential risks. These risks can include cyber-attacks, insider threats, and equipment failure. Fauzi and Lubis (2021) added that ISO/IEC 27005 provides a framework for risk management by prioritizing planning, execution, validation, and action. This framework, along with similar others, helps create a standardized approach to quantify and qualify risks accurately, thereby facilitating the creation of a DRP.

Kawtar et al. (2020) emphasized the importance of BIA because it provides insight into business and IT alignment changes. Alomoto et al. (2021) noted that changes may occur due to the social, environmental, and economic impact of business decisions (Alomoto et al., 2021). Using BIA, organizations can align sustainable development strategies and adopt business intelligence (BI) to enhance their competitive edge (Chi & Mahmud, 2020). Assessing the alignment supports key business elements, including

innovation, agility, adoption, and supply-chain support. Finally, business analytics is another core component that allows data processing and knowledge conversion to improve enterprise efficiency (Alnoukari, 2021; Vinnychuk et al., 2022). As each author implies, BIA is crucial in developing DRP because its information provides a pathway to create an efficient alignment of IT and business to recover from a disaster.

Policy creation and awareness training, or Governance and Guidelines, are designed by leadership, managers, human resources, and IT management to protect the company's information assets, property, and employees (Darmansyah et al., 2020). Ovrutsky (2020) noted that these policies help manage the creation, dissemination, and use of information, which is then influenced by communication concepts and training. Baizat et al. (2022) noted that these programs emphasize awareness and mitigation strategies to prevent potential negative impacts of IT, such as distractions and errors that could lead to cyberattacks and equipment damage. The goal behind policy creation and awareness makes it a crucial step in addressing the IT portion of the DRP, as BIA addresses the alignment.

However, complications can arise due to ethical and value issues, so documents must clearly state all information related to policy development. Ayeni et al. (2021) stated that the reason for the clarity is that implementing policy strategies directs organizational goals for controlling potential shortfalls and deviations from policy targets. Another significant impact is legislation on culture and privacy policy, which can alter organizational policies to ensure compliance (Stetsenko, 2021). Despite these

challenges, Wang (2021) emphasizes the importance of these policy processes in addressing future threats.

There are challenges in critical documentation and data backup processes. These processes restore critical data after a catastrophe, which allows an organization to continue conducting business (Higashi et al., 2020). However, Higashi et al. explained that the interdependent chain of custody and digital environment preservation does not give sufficient importance to reliable systems with sufficient capacity to archive records. This issue impacts DRP strategies due to the growing demand for data storage and analytics (Savita & Verma, 2020).

Resource planning or a development plan involves project management, user involvement, infrastructure development, human resources, and resource utilization. The planning ensures that IT has the necessary resources to operate successfully within an organization (Sutrisno et al., 2023). Sutrisno et al. also concluded that increasing IT proficiency would help sustain profit-oriented organizations. Putri et al. (2021) note that the process involves collaboration and constructive interaction among development actors in infrastructure planning. Furthermore, Ngala (2021) emphasized the necessity of user involvement in enterprise resource planning implementation, while Grod et al. (2022) and Irawan (2023) highlighted the importance of utilizing mathematical models and human resource management to enhance the effectiveness of work planning and performance improvement. These processes help create a comprehensive IT, DRP that outlines roles, responsibilities, communication protocols, recovery procedures, and a timeline for each process (Kesa, 2023).

Testing and maintenance procedures ensure the reliability and functionality of software and hardware systems. Software maintenance procedures, technical inspections, and defect detection are essential procedures that confirm the intended functionality of software modules, identify defect parts, and facilitate program repair (Jahangiri et al., 2020; Kumar, 2023; McDermott & Hatemi, 2020). A DRP must be tested through simulations and exercises to locate weaknesses, refine products and plans, and provide a focus on training personnel to ensure a coordinated approach during an actual incident (Kesa, 2023). Training ensures a clear understanding of the roles and responsibilities involved in DRP execution. The training will include incident response procedures, data protection, and IT resilience.

The risk of data loss, server failures, fires caused by overheating servers, cyberattacks, and insider threats necessitate following the DRP creation process and execution (Shetty et al., 2022). However, failure to follow the creation processes can cause an alignment issue between recovery strategies and management's vision of business processes (Houtkin, 2024). Abualkishik et al. (2020) added to this by stating that leaders should consider DRP and business requirements after mapping out these processes to determine if both processes can operate together. Therefore, Putri et al. (2021) noted that IT leaders should consider DRP a critical business process. Therefore, these leaders should utilize the aforementioned processes. Houtkin (2024) concluded that aligning DRP with business requirements should occur after assessing critical business processes, such as ISO/IEC 27005.

Disaster Recovery Plan Challenges

When considering DRP, it is necessary to consider the hindrances associated with its implementation. First among these challenges would be the cost of developing and maintaining an IT recovery plan, which may challenge budgetary constraints. Disaster recovery also requires testing, which involves having hardware, software, personnel, third-party experts, and time to simulate and evaluate scenarios for the plan's validity. Moreover, a plan often involves a secondary site with enhanced redundancy (Angafor et al., 2023). A potential solution for reducing costs is to offload them into a cloud-based DRP, which alleviates some of the burdens listed above. Abualkishik et al. (2020) claimed that cloud-based DRP was the least expensive compared to other alternatives, which can help control and help with elastic scalability. Elastic scalability can add and subtract resources as needed, thereby controlling costs and waste that the organization would otherwise incur. Aligning DRP with these regulations requires time and effort, accompanied by robust data backup, recovery, and security measures that can handle the load and comply with data protection regulations.

While cloud computing can present solutions for DRP, there are considerations for organizations. The main one is the lack of direct data control. While the shared responsibility model places the responsibility of data on the organization, in most cases, all cloud service providers (CSPs) are third-party vendors. This fact creates a dependency on CSPs for on-site data management. A secondary issue is if a CSP subcontracts with another vendor for data storage, which can increase the risk of data loss (Abualkishik et al., 2020).

The other significant challenge involves organizations with complex and interconnected IT infrastructures that pose challenges to DRP and BCP (Kesa, 2023). Mapping all interconnections and dependencies poses a challenge to developing and maintaining both plans. The Internet of Things (IoT) introduces even more complexity to the systems and increases the number of potential attack avenues (Staddon et al., 2021). The more complicated the network, the more time and resources are needed to follow the steps to build a DRP mentioned above.

Business Continuation

BCP refers to planning and implementing strategies to ensure the business continuity of IT systems and services during a disruptive event (Kesa, 2023). IT BCP aims to minimize data loss, downtime, and service disruptions, thereby maintaining critical IT and company functions and supporting them. The BCP lifecycle is essential for organizational resilience following a disaster, which was tested during the COVID-19 lockdowns, prompting businesses to develop contingency plans to adapt to at-home orders (Irkey & Tüfekci, 2021; Ramakrishnan, 2022). Additionally, these strategies can help ensure the continuation of critical services to prevent life-threatening situations in facilities like hospitals during disasters (Connolly et al., 2022; Ramakrishnan, 2022; Wisniewski et al., 2023). These strategies include redundancy and failover, data backup and recovery, disaster recovery sites, cloud services, incident response, cyber security measures, supplier and vendor management, staff training, and awareness (Kesa, 2023).

While BCP seems similar to DRP, the differences involve the availability of IT systems and services, data protection and recovery, infrastructure resilience, incident

response, business continuity integration, vendor and supplier management, testing and exercises, and continuous improvement (Irkey & Tüfekci, 2021). The availability of IT systems and services ensures the continued storage, communication, and delivery of applications (Kesa, 2023). IT ensures availability and accessibility to users by implementing redundant systems, load balancing, and failover mechanisms, thereby minimizing downtime and ensuring continuous service (Russo et al., 2023). Without these measures, organizations cannot maintain these functions during or after a disaster.

BCP and DRP in the Cloud

Data protection and recovery help businesses safeguard and restore all data critical for an organization to continue operations as usual (Kesa, 2023). However, issues like insufficient cybersecurity, integrity, reliability, and accessibility can hinder this process (Plaka, 2022). Organizations attempting to deliver robust backup systems, DRP, and secure data storage evaluate cloud computing due to its cost-effectiveness, elastic scalability, and reliability (Abualkishik et al., 2020). Furthermore, there has been a focus on data protection with a multi-cloud strategy.

Multi-cloud deployments involve utilizing multiple cloud services within a single heterogeneous architecture, offering enhanced flexibility, resilience, and performance compared to a single cloud solution (Mamidi, 2024; Shrivastava et al., 2023). Risk reduction and increased flexibility can be achieved by spreading workloads across multiple providers and allowing them to be switched between (Mamidi, 2024; Merseedi & Zeebaree, 2024). Organizations can recover data and operations more efficiently after an outage by ensuring a seamless switchover from a failed server, thereby maintaining

near-uninterrupted availability (Olorunyomi et al., 2024; Voruganti, K.K., 2024).

Furthermore, multiple copies of data spread across different cloud environments provide efficient redundancy in the event of a disaster (Tabassum et al., 2023). Finally, multi-cloud deployments can range from as simple as multiple software-as-a-service (SaaS) solutions to as complex as distributing applications across different cloud service providers (Shrivastava et al., 2024).

Voruganti (2024) suggested best practices that include cloud orchestration tools, optimization techniques, and governance models. Additionally, they highlighted the importance of this for optimizing resource deployment and management across diverse environments. Organizations utilize cloud orchestration to establish a workflow of automated tasks necessary for managing connections and operations within the cloud, enabling them to perform business functions (Alabdullah et al., 2020; Rashed Gaber & Elsamadicy, 2021; Rowlands, 2021; Voruganti, K.K., 2024; Xue et al., 2022). Chen et al. (2021) described cloud governance models as implementing, defining, and monitoring framework policies that guide an organization's cloud operations. The framework typically extends existing IT practices to fit the rules and policies necessary for a cloud environment (Zwitter & Hazenberg, 2020). Kartashov and Globa (2024) defined cloud cost optimization as determining an effective method to allocate cloud resources to maximize performance while minimizing costs.

Organizations use this solution to prevent cloud sprawl, which Kartashov and Globa (2024) defined as an uncontrolled proliferation of an organization's cloud services, instances, Khan et al. (2024) stated that lack of visibility and control is a common cause

of this issue, Without proper monitoring and management, organizations may lose visibility into their cloud infrastructure, making it challenging to identify and address potential issues during a disaster recovery scenario (Ibrahim, 2024). An example includes different teams within an organization independently deploying various cloud services without central management, which creates a disorganized cloud ecosystem with redundant subscriptions and potential security vulnerabilities (Abualkishik et al., 2020). This process can lead to significant cost overruns and potential security inconsistencies among different services and providers, which challenge the goals of DRP and BCP.

Cloud governance, centralized cloud management, and regular audits are methods to mitigate cloud sprawl. Implementing clear guidelines for cloud service usage, including approval processes for new subscriptions and resource allocation, could address issues such as vendor lock-in and data sovereignty (Amajuoyi et al., 2024). A single cloud management platform also improves visibility and control over cloud resources. Moreover, a single platform consolidates data from multiple cloud environments, providing a comprehensive view of resource utilization and identifying potential areas for optimization (Kesa, 2023). Finally, periodic reviews can identify unused and underutilized cloud services, which can help IT optimize services to reduce cloud sprawl (Ibrahim, 2024).

Tabassum et al. (2023) noted that benefits come with security challenges related to data security, privacy, and trust in multi-cloud deployment. For example, data security faces concerns such as confidentiality risks and virtual machine attacks (Kesa, 2023).

Tabassum et al. (2023) noted that methods to address these issues include end-to-end encryption, access controls, and data anonymization.

Data privacy strategies prioritize safeguarding data in the cloud from leakage, loss, or misuse through breaches (Mustafa et al., 2022). Prioritization is essential to maintain customer trust, prevent data breaches, and ensure regulatory compliance with laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) (Suganya & Sasipraba, 2021). Suganya and Sasipraba emphasized the importance of encryption, privacy by design principles, data access control, and inventorying sensitive data as essential steps to ensure privacy protection within a multi-cloud environment.

Singh et al. (2021) described trust in multi-cloud services as a commitment and approach taken by cloud service providers to ensure their platforms are secure, private, compliant, resilient, and respectful of intellectual property. The challenges of trust management include centralization and single-point failures. The High-Availability and Integrity Layer (HAIL) and machine learning-based trust verification help maintain trust within a cloud environment (Naidu et al., 2021; Saleem et al., 2021).

Overall, a multi-cloud strategy significantly enhances data protection and recovery for business continuity by distributing data across multiple cloud providers, creating redundancy and minimizing downtime in case of a single provider outage or disaster, effectively ensuring access to critical data even during disruptions; this also helps avoid vendor lock-in and allows businesses to leverage the best features of each cloud platform for optimal data management (Naidu et al., 2021).

Resilience

Infrastructure resilience refers to an IT infrastructure that can withstand disruptions and efficiently recover from malfunctions or failures (Kesa, 2023). This process involves building infrastructure with redundancy, scalability, and fault tolerance, while implementing maintenance and monitoring practices to detect issues before they occur (Angafor et al., 2023). Outside of technology, resilience can be achieved by creating a blame-free culture that follows a metric-driven approach, while encouraging routine performance outage drills.

A metric-driven approach in disaster recovery and business continuity involves assessing organizational maturity and implementing comprehensive frameworks to ensure resilience (Kesa, 2023). This approach utilizes quantifiable data points to inform decisions about systems or organizational performance (Russo et al., 2023). This measure will allow for a more objective approach to business continuity management.

BCM encompasses planning for the swift resumption of critical operations after disruptions (Huapaya-Ruiz & Meneses-Claudio, 2024; Russo et al., 2023). Key components include IT Disaster Recovery Planning, risk assessment, and the development of robust recovery strategies (Kesa, 2023). Maturity models provide a means to evaluate BCM implementation (Pinto et al., 2022), while stakeholder analysis is crucial for successful Area-BCM (Sapapthai et al., 2020).

Performing outage drills in DRP and BCP offers significant benefits for organizations. Scenario-based exercises, such as virtual incident response tabletop exercises, enhance cybersecurity awareness among managers and IT professionals

(Angafor et al., 2023). It enables organizations to identify weaknesses in their plans, test their response procedures, and ensure that employees are prepared to react effectively during a disaster, while minimizing downtime and protecting critical business functions (Sasaki et al., 2020). These drills enable businesses to evaluate and improve their incident response and disaster recovery procedures, including communication flows and decision-making processes (Angafor et al., 2023).

Regular testing of BCP is crucial to ensure their effectiveness, with 44% of studies suggesting continuous plan testing (Huapaya-Ruiz & Meneses-Claudio, 2024). Outage drills help organizations identify gaps in their existing processes and develop strategies to prevent future threats (Angafor et al., 2023). Additionally, these exercises contribute to developing integral and universal components for hospital BCP, such as alternative methods and resources, priority of operations, and resource management (Sasaki et al., 2020). Overall, outage drills play a crucial role in enhancing an organization's resilience and preparedness for potential disruptions. Incident response is an organizational action to handle a cyberattack, which Green (2023) stressed as necessary, as response time is critical. These actions include preventing, detecting, mitigating, responding, and recovering from a cyberattack (Angafor et al., 2023). When performed expediently, an incident response will mitigate damage from an attack and ensure business continuity (Angafor et al., 2023). Angafor also stressed that reducing response time reduces costs and recovery time, mitigates reputation damage, identifies root causes, and evaluates best practices.

Incident response is an organizational action to handle a cyberattack, which Green (2023) stressed as necessary, as response time is critical. These actions include preventing, detecting, mitigating, responding, and recovering from a cyberattack (Angafor et al., 2023). When performed expediently, an incident response will mitigate damage from an attack and ensure BCP (Angafor et al., 2023). Angafor also stressed that reducing response time reduces costs and recovery time, mitigates reputation damage, identifies root causes, and evaluates best practices.

BCP integration helps organizations prepare to respond to disruptions, such as economic downturns, natural disasters, or cyber-attacks; however, a plan needs to be integrated with the company's goals and projections (Kamarudin et al., 2024). The benefits of the integration are minimizing damage, maintaining operations, empowering employees, building trust with the clients, and ensuring continuous compliance. The integration must encompass a comprehensive understanding of the critical areas of the IT system and the organization's critical services to identify recovery priorities (Russo et al., 2023). The chief information security officer (CISO) must guide the stakeholders during the benefit-cost ratio (BCR) and BCP implementation to understand what must be achieved to comply with company goals and regulations.

Integrating a BCP into DRP provides a comprehensive strategy to minimize disruption and ensure an efficient return to normal operations by aligning IT systems restoration with broader organizational recovery plans. Components for effective BCP include alternative methods and resources, prioritization of operations, and resource

management (Sasaki et al., 2020). An example of alternative methods and resources includes implementing multi-cloud solutions, as mentioned above.

Maturity models can assess an organization's implementation of business continuity frameworks (Pinto et al., 2022). These models offer organizations a systematic approach to assessing and enhancing their capabilities by evaluating their current state, developing future visions, and comparing capabilities across organizations (Mazimwe et al., 2021). Adekunle et al. (2022) noted that it could also help support IT infrastructure management through configuration management, which has planning challenges that Kesa (2023) identified as emerging technology and organizational resistance. Using this framework can improve the pathway to an effective BCP and DRP.

Intelligent process automation significantly enhances DRP and BCP by improving efficiency, reducing costs, and mitigating risks (Brás et al., 2023). Geospatial analysis, remote sensing, and machine learning enable organizations to make informed decisions while facilitating efficient response operations (Abid et al., 2021; Luo et al., 2020). Machine learning and deep learning methods are utilized in disaster management, including prediction, risk assessment, early warning systems, and damage assessment (Linardos et al., 2022). Automating these services increases the integration of BCP and DRP.

Integrating lean and resilience paradigms further enhances an organization's ability to maximize value while minimizing waste and dealing with risks (Habibi Rad et al., 2021). Sustainability and resilience capabilities also contribute to effective BCM

(Corrales-Estrada et al., 2021) by emphasizing a multidisciplinary approach to organizational preparedness (Russo et al., 2023).

Vendor and supplier management ensures meeting supply chain issues during a disaster (Kamarudin et al., 2024). Strategies involve Several components, including service level agreements, vendor-business continuity plans, diversification of suppliers, vendor risk management, leveraging technology, establishing transparent communications channels, conducting regular audits, and continuous risk assessments to keep the network safe (Kesa, 2023). Adenekan et al. (2024) include adopting international cybersecurity standards and frameworks, integrating advanced security technologies, and continuously monitoring the IT portion of supply-chain issues that might arise from disasters. While these processes exist, they can become complex because not all vendors or suppliers use the same systems, which may lead to conflicts when implementing this plan (Kamarudin et al., 2024). Therefore, plans need to account for those occurrences to minimize disruption.

Like DRP, testing and exercise are vital because they increase the plan's readiness. Scenario-based incident response exercises raise cybersecurity awareness within the organization (Angafor et al., 2023). These activities also evaluate incident response and disaster recovery procedures to improve strategic decision-making and enhance the technical skills of cybersecurity personnel (Angafor et al., 2023). As threats evolve, as mentioned in this literature, there is precedence for the routine conduct of these scenarios to prepare for disruption.

Continuous improvement focuses on monitoring and evaluating the effectiveness of BCP strategies, processes, and plans. There are also post-training reviews and feedback to enhance productivity, quality, and customer satisfaction in the production area, as well as resilience (Abrahams et al., 2024). These measures are needed to adapt to evolving threats that organizations face.

Using the Framework with the Topic

The study examines IT personnel's strategies for implementing a disaster recovery plan in the Southeast United States. As discussed, there are various strategies to implement BCP and DRP; however, organizational resistance exists to their adoption. Therefore, I will use UTAUT to guide the development of interview questions and to discover IT personnel's strategies for overcoming these challenges when implementing BCP and DRP. Performance expectancy, effort expectancy, social influence, and facilitating conditions will serve as concepts to explore how these aspects affect the adoption of DRP and BCP.

Performance expectancy reflects the belief that technology or policy may affect their job performance (Venkatesh et al., 2003). Disruption of regular workflow can significantly impede job performance (Sert et al., 2023). Implementing these systems, such as infection prevention and control, can be time-consuming and uncomfortable for users as they adapt to their jobs, which negatively impacts their performance (Charoenthammachoke et al., 2020; Kesa, 2023). These factors collectively contribute to potential resistance to adopting DRP and BCP processes. Hashim et al. (2020)

recommend using frequent drills to familiarize users with the system, which may lower the impact on their performance.

Effort expectancy reflects the ease of use of a particular system. Employees tend to reject tools due to their complexity or irrelevance, which limits their use during a crisis and hinders recovery (Shatta & Mabina, 2024). Research indicates that employees may reject complex tools during crises, which can hinder recovery efforts. This can be attributed to limited training, poor infrastructure, and inadequate access to technology (Ntshwarang et al., 2021). Effective crisis management requires a balance between comprehensive and intuitive decision-making, with improvisational approaches often proving valuable in time-pressured situations (Tabesh & Vera, 2020; Okoli, 2020). However, organizations can mitigate these challenges by implementing user-friendly tools, such as augmented reality and artificial intelligence, to support less skilled workers (Szajna & Kostrzewski, 2022). To enhance employee well-being and performance during crises, organizations should focus on fostering a positive mindset and promoting organizational citizenship behavior (Pipera & Fragouli, 2021). Adopting flexible work arrangements and digital tools can help organizations and employees adapt to new challenges, although implementation may vary across sectors and countries (Raghavan et al., 2021).

Facilitating conditions include employees and staff believing support is available when they use DRP and BCP policies and technology. This process involves IT staff having a comprehensive understanding of IT infrastructure, risk assessment, and robust

recovery strategies, which enables them to explain how to (Kesa, 2023). Strategies to improve these conditions may enhance employee support for DRP and BCP.

Transition and Summary

The literature overviewed UTAUT, BCP, and DRP to explain how each will be applied to this study. I provided a foundation for UTAUT by examining how it is applied in the context of technology acceptance or policy adoption. I explored the concepts of DRP and BCP related to current and best practices while integrating them into the conceptual theory for use in the data collection phase.

Section three shall explain how I plan to collect data ethically. The research design shall include measures I plan to use to protect the participants while ensuring their rights are protected. It will also explain how I plan to collect, organize, and analyze the data, utilizing member checking and data saturation to ensure the reliability and validity of the study. These steps will serve as the basis for the analysis that will inform the presentation of the study and the recommendations based on the data in Section Four.

Section 3: The Project

Project Ethics

I was the primary data collection instrument in this study. Chai et al. (2021) stated that qualitative researchers collected contextual data to explore human behavior, attitudes, and beliefs. Chai et al. explained that qualitative researchers were responsible for collecting information through in-depth interviews, observation, and focus groups. Researchers must carefully consider the ethical aspects and construct appropriate tools for data collection, particularly when addressing sensitive topics (Tourish & Craig, 2025). The researchers carefully constructed data collection tools to ensure the robustness of their data collection. Therefore, I gathered data by conducting interviews with participants and collecting publicly available documents.

My experience with BCP and DRP was based on classes in higher education and personal discussions with IT managers before this study. I did not conduct interviews with anyone with whom I had a prior professional or friendly relationship to mitigate inappropriate influence on the research subject. I also controlled my bias by focusing on what participants and public documents stated about the subject, rather than relying on my previous knowledge. Controlling bias by prioritizing participant and second source input over the researcher's prior knowledge presented an objective view on the topic and avoided skewing information in a direction not repeated in research (Vaidyanathan, 2022; Pollock, 2020).

I protected participants by adhering to the principles outlined in the *Belmont Report*. The report, published in 1979, emphasized respect for people, beneficence, and

justice (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). This report was created in response to severe ethical breaches such as the Tuskegee Syphilis experiment, and it was necessary to follow the recommendations to protect the participants (Frye et al., 2021; Reyes, 2020).

Beneficence means minimizing harm and maximizing the benefit of the study. Justice was achieved because the benefits and risks were distributed equally among all participants (Office for Human Research Protections [OHRP], 2022). I minimized risk in the data collection by ensuring that participants remained anonymous and that all questions did not include psychological or emotional trauma amongst the participants. Each participant received the same questions and benefited equally from the process.

I completed the Collaborative Institutional Training Initiative (CITI)'s Human Subject Protection Training. This training reviewed the concepts of the Belmont Report and other ethical measures necessary for conducting research with human participants. The certification could be found in Appendix A.

I received authorization from the Walden University Institutional Review Board (IRB) with approval number 03-24-25-1146259. The IRB ensured ethical compliance and reviewed protocols before and after approval (Cox et al., 2021; White, 2020). The IRB adheres to these principles, specifically that all participants have autonomy, act to benefit others while protecting their welfare, and distribute risk and benefits equally for the research before collecting data (Reyes, 2020).

Fundamental ethical principles included obtaining informed consent, maintaining confidentiality and anonymity, respecting cultural sensitivities, and avoiding harm to

participants (Ghimire, 2021). Laryeafio and Ogbewe (2023) focused on addressing power dynamics, facilitating authentic expression, and preventing tokenistic participation. Facca et al. (2020) also highlighted additional considerations, including data handling, privacy concerns, relational ethics, respecting cultural norms, and providing support after the study.

Protecting the participant's privacy was paramount, and I avoided anything that identified them (see Dougherty, 2021). I avoided PII in the interview questions, such as name, personal identification numbers, physical address, or other identification details. I followed the interview protocol (see Appendix B) to ensure that I did not socialize with PII. I also obfuscated any mention from the recording and transcript if it was accidentally mentioned. Finally, I used pseudonyms to identify quotes associated with emergent themes when presenting the findings, such as "A1" and "A2."

Interview responses, transcripts, and audio recordings will be stored on an encrypted flash drive in a secure lockbox for a period of 5 years. Facca et al. (2020) emphasized that researchers must take the necessary steps to prevent unauthorized parties from accessing data. Any physical documents stored in a locked cabinet are only accessible to me. Furthermore, I used my secured laptop exclusively for data collection and analysis to minimize data leakage to unauthorized individuals. Finally, I limited coercive invitations by not including incentives as a recruitment strategy.

I adhered to voluntary participation throughout the data collection and participant recruitment process. The first step was to use the informed consent process, which included explaining the study's aim, objective, purpose, benefits, and risks associated

with the study to the potential participant. I also disclosed my identity as the researcher, the purpose of the research, and the affiliated institution. I also informed them of their right to refuse or withdraw from the study at any time without any repercussions. Even after being informed of consent, I reminded the participants of their rights before conducting the interview. The participants consented by sending a response email with “I consent,” after which I arranged an interview time. I gave each participant two weeks to read and respond to the informed consent process. During that time, I was available to answer any questions related to the study.

I retained all data on the flash drive and in a locked cabinet for up to 5 years. After that period had elapsed, I digitally erased all information on the flash drive using a program called File Shredder. This program deleted files, making recovery improbable. I shredded all physical documentation as well. This process ensured that I retained the data as mandated and disposed of it properly after that period elapsed.

Nature of the Study

I used the qualitative method to answer the research question. Qualitative research enabled the in-depth exploration of complex social phenomena and human experiences, providing rich and detailed data. Additionally, it provided an understanding by applying “how” and “why” questions, which gave context to the answers (Denny & Weckesser, 2022; Tuckerman et al., 2020). I chose a qualitative methodology because I wanted nuanced answers about DRF and BCP adoption.

Research Method

I employed a qualitative research study to investigate participants' beliefs, feelings, ideas, and opinions regarding a central problem, which was expressed in words rather than numbers (see Tanwir et al., 2021). Qualitative methods offer an in-depth understanding of phenomena, providing answers to "how" and "why" questions (Tuckerman et al., 2020). An advantage of the qualitative research methodology is that it is more responsive and flexible, utilizing interviews to collect visual images or text, which provide rich sources of insights, compared to the quantitative research methodology, which focuses on analyzing numerical data through surveys (Denny & Weckesser, 2022). By employing qualitative research, I gained insight into people's perceptions. In this study, I explored IT leaders' strategies for implementing DRP and BCP after a cyberattack; therefore, I selected the qualitative method as the most relevant approach. I employed the qualitative method, based on the study's primary research question. I employed qualitative research, focusing closely on the human experience, to provide researchers with process-based, storied data on a phenomenon (see Taherdoost, 2022).

Research Design

I used pragmatic inquiry to study this phenomenon. I used this design because it emphasized flexibility by the industry rather than analyzing a particular case (see Tuckerman et al., 2020). This design enables the recruitment of individuals with direct experience in the research topic through social media, thereby increasing access to participants (Capps, 2023). Pragmatism in industrial marketing research emphasized

developing adaptable solutions to practical problems (Lowe et al., 2020). Moreover, this approach provided all the necessary tools to develop a deeper understanding of the strategies that IT leaders used to implement DRP and BCP after a cyberattack. Capps (2023) noted that pragmatic studies helped examine decisions by one or more people in an actual situation. The process included identifying the problem and leading inquiries that helped comprehend and resolve it. The results led to recommendations for policies, new environmental projects, or societal transformations (Capps, 2023).

I used a pragmatic inquiry research design because it is frequently employed in qualitative research, as it offers a flexible and accessible theoretical approach for conducting research (Ngenye & Kreps, 2020). Interpretive description was an alternative research design because it could address complex experiential questions that generated practical outcomes. The pragmatic inquiry distinguished itself from other qualitative approaches by focusing on generating knowledge and understanding (Hussain et al., 2020). The pragmatic inquiry approach yields an interpretive account, created through iterative and critical examination of a topic (Lazem & Sheikhtaheri, 2022). It helped the researcher understand the studied experience without surrendering the methodological integrity of qualitative approaches (Taherdoost, 2021). Thorne's (2016) interpretive description methodology converted the collected data into patterns and reorganized them into themes to answer clinical questions (Stevens et al., 2021). Characteristics, patterns, and structure can help process specific contexts to generate strategic paths for building knowledge through retroactive reflective interviewing, cross-sectional reporting, or

longitudinal follow-up (Thorne, 2016). Therefore, this research validated the credibility of the study's findings using pragmatic qualitative inquiry.

Population, Sampling, and Participants

The population for this pragmatic inquiry study comprised experienced IT managers who had at least 10 years of experience in cloud computing technology and in implementing DRP and BCP, and who worked in several information technology companies in the Southeast United States. These managers have experience implementing DRP and BCP programs, as well as managing teams with three or more members. Participants were current or former IT DRP and BCP implementers who had experienced different project outcomes. Pung and Rienhoff (2020) preferred to choose participants with experience in the subject matter, as this would provide more information about the phenomenon. This choice served as the basis for my population. Furthermore, the participants must have been involved in various IT projects, including aligning business and IT, implementing IT strategy, conducting technology research, and executing strategic initiatives.

I formed a working relationship with participants by clearly communicating with them during the research process. Gallegos et al. (2023) stated that clear communication on research purpose and expectations fosters a positive working relationship. I used the informed consent process to facilitate this action and answered any questions a participant might have had. Furthermore, I summarized the informed consent before the interview to ensure the research objective was transparent to the participant.

I also used active listening to demonstrate a genuine interest in their experiences. Rowlands (2021) stated that showing an interest in the participant's information helps keep the participant engaged and comfortable with the interview. I listened intently to the participant's statements and asked follow-up questions to clarify any points that required further explanation.

Finally, I was mindful of their time commitments outside this research study. Hodge et al. (2020) noted that they should offer flexibility in scheduling to accommodate their schedules. Additionally, Hodge mentioned that the scheduled time and interview length should be honored. I offered flexibility in scheduling to ensure I met with all potential participants at their convenience. Furthermore, I adhered to the time constraints agreed upon by the participants and notified them when they reached the 30-minute mark of the 40-minute time limit. This mention allowed them to end the interview or allow additional time beyond what was stated in informed consent.

The participants were required to be involved in IT projects, including aligning business and IT, implementing IT strategies, conducting technology research, and executing strategic initiatives. The sample size in qualitative research was typically determined by theoretical saturation rather than predetermined numbers (Chai et al., 2021). From this population, I used purposeful sampling to gather four participants from LinkedIn and member listings from HelpDesk Chapters (HDC), the Association of Independent Information Technology Professionals (AIIP), and the Association for Information Systems (AIS) because I had reached data saturation. Purposeful sampling is a non-probabilistic technique commonly used in qualitative research to select participants

based on specific characteristics relevant to the research question (Chai et al., 2021; Nyimbili & Nyimbili, 2024). This method was suitable for this study because I selected specific industry members with the necessary experience to answer the research question.

Data saturation was reached when no new information existed, and further coding was no longer feasible (Fusch & Ness, 2015). Researchers in these situations found redundancy in the collected information, indicating that data collection could be concluded (Trener et al., 2021). Failure to reach data saturation impacted the quality of the research and compromised the content validity of the study (Fusch & Ness, 2015). After each interview, I reviewed the transcript for new codes to include in the themes. I had reached data saturation if no new codes were generated or if any were repeated from previous interviews.

Data Collection Activities

I served as the instrument by conducting semi-structured interviews and collecting publicly available documents related to the research question. Interviews have become valuable tools for IT research, offering cost-effective and broad-reaching data collection methods (Artykutsa & Prokhorova, 2021; Holovnia et al., 2023).

I served as the instrument by conducting semi-structured interviews and collecting publicly available documents related to the research question. Interviews have become valuable tools for IT research, offering cost-effective and broad-reaching data collection methods (Artykutsa & Prokhorova, 2021; Holovnia et al., 2023). A semi-structured interview offered flexibility in communication when exploring rich data, providing open-ended questions that allowed for a thorough exploration of the topic (Saleem et al., 2021;

Thunberg & Arnell, 2021). This method was enhanced using an interview protocol, which guided interviews with open-ended and follow-up questions (Brás et al., 2023). I used the interview protocol to facilitate each interview (see Appendix B). Finally, I collected peer-reviewed journal articles from the Walden Library and other publicly available industry-related documents for documentation. These documents served as a secondary source for triangulation.

My first step was to obtain IRB approval. Second, I invited prospective members from the population and engaged in the informed consent process with those who replied as described in Project Ethics. I scheduled a 30- to 40-minute interview via Zoom at a time convenient for them and used the interview protocol (see Appendix B) to conduct it. The process involved conversing with the participant to gain knowledge of the topic (Tanwir et al., 2021). I recorded only the audio for the interview to protect the participant's privacy. I also made observations to aid in my interpretation of their answers. Qualitative research observations included descriptions of the research participants, physical settings, and details about the activities and events related to the research topic (Elias, 2024).

I ensured the reliability and validity of the study by performing member checking. As a researcher, I reviewed my interpretations with the participants to ensure that they aligned with their intended meanings for a particular answer (Rowlands, 2021). I performed this by conducting a second 15-30 minute interview to review my analysis of the first interview, and allowed them to clarify any inaccuracies. Once I gathered their answers, I transcribed and updated the information to enhance my data analysis process.

Interview Questions

1. From your experience in cloud computing, what cybersecurity strategies would you use to implement DRP and BCP after a cyberattack?
2. Based on your experience in IT, have you ever participated in any DRP and BCP implementation after a cyber-attack? #Please describe the experience that would be a follow-up.
3. From your experience implementing DRP and BCP, what are the key barriers that you have encountered while implementing DRP and BCP after a cyber-attack on an organization?
4. Based on your past experiences in cloud computing, what steps do you take to ensure DRP and BCP policies will not interfere with job performance?
5. From your past experiences in IT, what steps do you take to simplify the execution of DRP and BCP?
6. Based on your past leadership experiences, how would you mitigate potential outside attitudes toward a particular DRP or BCP policy?
7. Based on your past leadership experiences, how would you improve the attitude toward DRP and BCP so staff may adopt these policies?
8. From your experiences in cloud computing, what importance do external factors, such as laws, regulations, and privacy, play in implementing a DRP and BCP after a cyberattack?
9. Based on your past experiences in cybersecurity, what additional strategies would you use for implementing DRP and BCP after a cyberattack?

Data Organization and Analysis Techniques

Automated transcription services and digital interview methods offer cost-effective solutions for researchers. Also, they maximized scientific utility and promoted transparency (Bull & Bhagwandin, 2020). I prepared the data for analysis by organizing interview transcripts, audio recordings, and research notes. After recording the interviews, I saved each record by assigning them alphanumeric participant names such as A1 and A2. Assigning a label to each interview helped organize it in a meaningful way (Sarfaraz et al., 2022). I then used Zoom Transcription to transcribe the interview and ensured its accuracy by reviewing the recordings against the transcriptions. Zoom transcription was part of the broader field of telepsychiatry and videoconferencing, which became increasingly prevalent during the COVID-19 pandemic (Gnanapragasam et al., 2021). Zoom offered a variety of transcription services, including live transcription, cloud recording, and AI-powered meeting summaries.

As Campbell et al. (2021) suggested, I used a research log to record the study process, situations, ideas, and new experiences during the data collection phase. A log-enabled correlation and arrangement allowed researchers to identify themes and research topics commonly used (Yoon & Chae, 2022). Therefore, I used these logs to organize the data for analysis.

I stored these items on an encrypted external hard drive, which I kept in a key-locked file cabinet when not in use. I retained these files for 5 years, as required by Walden University. After 5 years, I will use File Shredder to dispose of the digital files, as discussed in Project Ethics. Additionally, I will also shred all physical records.

I used data triangulation. This process collected data from various sources, including interviews and documents, to enhance the credibility and validity of the research findings (Vivek et al.; Yogarajah et al.; Sarmatha, 2023). Triangulation accurately reflected the phenomenon investigated by comparing diverse sources (Christou, 2022). The process involved comparing statements made by the participants with peer-reviewed journals and industry-related documents to ensure the accuracy of the findings (Liang et al., 2020). I used the semi-structured interviews and publicly available documents to triangulate and enhance the validity and reliability of the study.

I employed thematic analysis, as noted by Fuchs (2023), which is used to identify patterns in qualitative data and generate themes. The process began by familiarizing myself with the data through reading and re-reading transcripts, field notes, and other qualitative materials to gain a deep understanding of the content and identify initial impressions of potential themes. Then, I continued by generating the initial codes, which involved systematically breaking down the data into smaller units and assigning descriptive labels or codes to capture key concepts, ideas, or significant elements within the text. I used NVivo to search for recurring patterns and group them to generate themes. Then, I reviewed the themes by examining how they related, ensuring they were distinct, and verifying consistency across the dataset. Lastly, I defined and named the themes by clearly articulating the core meaning of each theme, providing a concise description and label that accurately represented the pattern identified in the data (Cernasev & Axon, 2023).

The data organization tool I used was qualitative data analysis software, such as NVivo, T-Lab, or KNIME, to facilitate coding, theme development, and visualization (Gede & Kawiana, 2023). I did not forget about Inductive and Deductive Coding. Inductive meant developing codes directly from the data without predetermined categories, allowing themes to emerge organically. Moreover, deductive coding was employed, utilizing pre-established codes based on the research questions to guide the analysis.

Study Validity

Unlike quantitative research, qualitative research discusses reliability and validity (Kakar et al., 2023). Trustworthiness in qualitative research was evaluated through the criteria of credibility, transferability, dependability, and confirmability. Because these criteria could not be directly measured, they had to be established using qualitative methods, such as triangulation and member checking (Paraskevaidis & Andriotis, 2023).

Reliability

Reliability in qualitative research refers to the consistency, trustworthiness, and dependability of the research findings (O'Connor & Joffe, 2020). I enhanced dependability by performing triangulation and member checking. Anufriyeva et al. (2020) described triangulation as the use of multiple data sources to corroborate findings from different perspectives, which ensured the accuracy of statements provided by participants. I compared the interviews with publicly available documents, including peer-reviewed journal articles from the Walden Library databases and other industry-

related documents. I used these in conjunction with the interviews to increase the reliability of the findings.

Member checking involved sharing preliminary findings with participants to confirm that they aligned with what they had stated during the interview (Kleinheksel et al., 2020). Member checking had to be included in the informed consent process so the participant knew it was a step in the research process (Soysal & Turkmen, 2024). I ensured that member checking was part of the informed consent and reminded the participant of this step during the interview.

After creating transcripts of each interview and a summary of my interpretations, I contacted each participant to schedule a ten-minute member-checking session through Zoom. During this meeting, I gathered feedback on anything the participant noted needed correction. Once the session was complete, I incorporated the feedback while discussing the themes that emerged from the interviews.

Validity

Validity in qualitative analysis, encompassing credibility, transferability, dependability, and confirmability, was a multifaceted concept that ensured the trustworthiness and rigor of the findings (Kakar et al., 2023; Guest et al., 2020). According to these authors, validity embodied the truthfulness of research data. Moreover, validity was achieved through participatory, intersubjective, analytic, contextual, emphatic, and ethical lenses (Stenfors, Kajamaa & Bennett, 2020). Additionally, I used data saturation to ensure that no further information was obtained from the interviews and that the answers were reliable and consistent. Fusch and Ness

(2015) noted that data saturation occurred when no new codes or themes were generated during the analysis of a data source. I reviewed the transcripts to identify new codes and additional themes. If new codes and themes were identified, I sought out additional participants to interview until no further information was gathered.

Data saturation was reached when no additional information was available, and further coding was no longer feasible (Fusch & Ness, 2015). Researchers in these situations found redundancy in the collected information, indicating that data collection could be concluded (Lu et al., 2021). Failure to reach data saturation affected the quality of the research and compromised the content validity of the findings (Fusch & Ness, 2015). After each interview, I reviewed the transcript for new codes to include in the themes. I reached data saturation when no new codes were generated or when codes were repeated from previous interviews.

Credibility

Credibility in qualitative analysis is critical to the trustworthiness, transferability, dependability, and confirmability of findings (Kakar et al., 2023). Moreover, credibility occurred when study conclusions could be viewed by researchers as credible, concerning the accuracy of results in relation to the reality of the topic investigated (Paraskevaidis & Andriotis, 2023). Strategies I used to enhance credibility included member checking of the data interpretation, triangulation, which utilizes multiple methods to assess the credibility of a study (Stahl & King, 2020), participant transcript review, interview protocol, focus group protocol, and more (Paraskevaidis & Andriotis, 2023).

Furthermore, I used Walden University's process approval to ensure the study's credibility.

Confirmability

Confirmability in qualitative research paralleled objectivity in quantitative research (Kakar et al., 2023). Moreover, it was considered a simplified quality criterion for trustworthiness in qualitative research (Megheirkouni & Moir, 2023). This referred to the degree to which research findings could be verified and trusted, particularly in qualitative studies (Kakar et al., 2023). It was based on strategies to enhance confirmability, including the use of standardized methods for data analysis, such as thematic analysis with a network approach, which allowed for scalability and verification (Chung et al., 2020). Simplifying quality criteria for qualitative research also helped gain academic confidence and trust (Megheirkouni & Moir, 2023). Confirmability was essential for ensuring the integrity of qualitative research, which often faced skepticism regarding its generalizability and objectivity. I ensured confirmability by maintaining a detailed audit trail that documented the research process, conducting member checks by sharing interpretations with participants for feedback, practicing reflexivity to acknowledge researchers' biases, and using triangulation by collecting data from multiple sources or methods (Hessels & Hooge, 2021; Roberts & Rosanne, 2020). I obtained confirmability in my research by generating transparent and detailed descriptions of my research collection, interpretations, analysis, and methodologies.

Transferability

Transferability in qualitative research refers to the degree to which findings could be applied to other contexts, settings, or populations (Younas et al., 2023). When transferability was employed, a thick description was essential for enhancing transferability, as it allowed researchers to assess the applicability of findings to different contexts, which was crucial for trustworthiness, credibility, dependability, and confirmability (Kakar et al., 2023). It was essential to demonstrate the relevance of the results to situations beyond the specific research environment studied; this was achieved by providing a rich and detailed description of the research context and participants, enabling readers to assess whether the findings could be applied to their own situation (Ahtisham Younas et al., 2023). For this research, I provided a comprehensive account of my research experiences, including details of the research practices and the data collection process. I promoted research transferability through context assumptions and explanations.

Transition and Summary

This section describes the project ethics and my role in the data collection process. I also clarified the qualitative pragmatic inquiry and defined the population, sampling method, interview processes, and validity. Section 4 presented the findings from this study.

Section 4: Application to Professional Practice and Implications for Change

In this section, I will provide the findings of this qualitative pragmatic inquiry.

The research question was: What strategies do some IT managers use to implement a disaster recovery plan? In this study, based on the four interviews conducted as described in Data Collection Activities, I developed three themes related to implementation: Implementation During Attack, Continuous Training, and Implementation Constraints. Table 1 includes a summary of themes, including their subthemes and relevant references.

Table 1

Summary of Themes

Theme	Sub-Themes	References
Implementation During Attack	45	2411
Continuous Training	50	1725
Implementation Constraints	30	1458

Before discussing the findings, it is essential to define DRP and BCP to clarify how these concepts address the research question. While they may sound interchangeable with disaster recovery plans, DRP and BCP serve distinct roles, as will be elaborated in the findings. DRP views the technical side, which includes the plans to respond to cyberattacks (Ibrahim, 2024). BCP, on the other hand, handles an organization's ability to continue after an attack (Ibrahim, 2024). While these may be considered plans to recover from a disaster, as stated in the research question, they will be discussed as DRP and BCP

to isolate which portion they respond to within the findings. This clarification is necessary to apply the findings to the following sections: Information Technology Contributions and Recommendations, Implications for Social Change, and Recommendations for Further Research, as well as to summarize the conclusions.

Presentation of the Findings

Implementation During Attack

I used the interview with participant A1 to demonstrate a structured methodology for incident response. In the interview with participant A1, I was able to highlight the importance of accurately identifying the event and evaluating its impact, including determining which systems and channels are affected, and promptly isolating the attack. The team employs alternative service delivery approaches such as shifting operations to another region or data center to sustain continuity during containment and solution development. To support readiness, A1 recommends regular reviews of response plans and practice scenarios. These strategies align with the research of Huapaya-Ruiz and Meneses-Claudio (2024), who endorsed recovery-enhancing methodologies and advocate for continuous contingency testing. Moreover, I found that companies underscore the significance of equitable recovery policies (Finucane et al., 2020)

Such practices exemplify the technical and organizational infrastructure described as facilitating conditions by UTAUT (Venkatesh et al., 2003), which refers to the supporting infrastructure that affects the acceptance of a particular technology. Establishing robust fail-safe systems that provide staff with access to essential resources and infrastructure increases their acceptance, as it ensures effective operations even in the

face of potential adverse events. Even in the face of adverse events. A1's approach demonstrates the tangible benefits of a well-crafted incident response plan that increases user engagement by supporting containment and operational continuity.

Additionally, the strategy also includes a link to performance expectancy and effort expectancy, which Venkatesh et al. (2003) described as a user perception that something will increase their job performance and the ease of use of the system. Continuous training and transparent, systematic procedures reduce the perceived complexity and cognitive burden during incident management, which helps increase the user's ability to perform their job effectively. This factor increases acceptance of recovery protocols by increasing the ease of use under pressure. Practice scenarios foster an organizational culture that helps standardize protocols among peers, aligning with the social influence that Venkatesh et al. (2003) attribute to the perception that peer opinions can influence the acceptance of technology. By standardizing the practice, the surrounding influences help promote consistent compliance with the incident response plan.

Participant A2 described disaster recovery as a series of concentric circles, highlighting the importance of implementing varying levels of protection for data and systems against potential failures and disasters. These graduated layers provide DRP and BCP alternatives, enabling continued operations even if one layer is compromised. Sasaki et al. (2020) illustrated that effective continuity plans incorporate alternative methods, operational priorities, resource management strategies, and supplementary resources.

This model aligns with the facilitating condition, which suggests that employees are more likely to utilize new systems effectively when essential infrastructure, such as hardware, software, and technical support, is readily available. In disaster recovery scenarios, the "system" refers to the overarching contingency plan. The concentric circles framework advocates for a resilient infrastructure with built-in redundancies and technical support to mitigate outages or disasters. This multi-layered methodology establishes the necessary conditions for sustained operations and encompasses organizational support, including resources and training for proper utilization of recovery systems. By developing and routinely testing the concentric circles plan, management proactively cultivates supportive conditions for its personnel.

Participants A3 and A4 emphasized the organization's ongoing reliance on cloud computing and backup solutions as a key strategy to mitigate the effects of a cyberattack. This methodology closely parallels the approach described by A1, who emphasized the adoption of alternative service delivery methods such as redirecting operations to different regions or data centers to maintain operational continuity while containment and remediation measures are underway. In alignment with A1's perspective, A3 also stressed the critical importance of promptly identifying essential systems and data. This allows for the prioritization of resources to protect what is most vital, ensuring that core business functions remain supported and that recovery efforts are focused where they are most needed. As such, this links to constructs of the UTAUT in a similar manner.

All interviewed confirm that all businesses are legally required to maintain a written disaster recovery plan to address a cyberattack, which includes the scope and

detail appropriate for the organization's size and industry. While specific requirements differ based on location and sector that contain unique laws and regulations, several common regulatory expectations include establishing robust data backup and recovery protocols, conducting regular testing and auditing of plans, defining clear organizational roles and responsibilities, implementing incident response procedures, and fulfilling data breach notification obligations. The National Institute of Standards and Technology (NIST) Cybersecurity Framework and the International Organization of Standardization (ISO) 22301 provide crucial guidance on meeting these legal requirements. Yamcharoen et al. (2022) emphasized the importance of cybersecurity laws in protecting critical infrastructure and sensitive information, while Bondoe et al. (2020) highlighted the NIST Cybersecurity Framework as a key regulatory framework. Abrahams et al. (2024) and Mantelero et al. (2020) further validated the importance of frameworks established by NIST and ISO, noting that these tools provide essential guidance for legal compliance. Regulations continue to vary by industry and location; however, these frameworks provide a structured pathway for organizations to follow. Analyzing this through UTAUT, the mandated requirements and frameworks have a significant influence on organizations' adoption of disaster recovery technologies. Industry standards and regulations exert a significant social influence within sectors, encouraging the adoption of comprehensive disaster recovery practices. However, these regulations also include necessary facilitating conditions, such as supporting infrastructures, adequate resources, and training. Both elements will influence employees toward adopting DRP and BCP as a whole within an organization.

Continuous Training

Participant A1 emphasized the importance of conducting semiannual reviews of DRP and BCP plans and practicing their implementation using real-world scenarios. Execution can be streamlined by maintaining comprehensive, clearly written plans and accessible knowledge articles at the service desk level. These strategies differ from the training mentioned in the theme implementation during an attack because they focus on response to scenarios rather than the ability to use systems. Angafor et al. (2023) advocated for the use of tabletop exercises to enhance strategic decision-making and develop both technical and soft skills within cybersecurity incident response teams. Additionally, virtual reality simulations offer a cost-effective and repeatable training solution that accurately models disaster scenarios and supports just-in-time learning (Jung et al., 2022)

Regular plan reviews enhance staff awareness of updated procedures, thereby increasing their ability to perform tasks effectively, which in turn contributes to performance expectancy. A review can also update knowledge articles to ensure they are complete and easy to follow, thereby reducing the effort required during high-pressure incident response. By increasing ease of use, as described in effort expectancy, staff are more likely to follow those procedures rather than outdated or complex ones that are difficult to follow. Additionally, the availability of these resources also helps increase the acceptance of the plans, which in turn facilitates the implementation of these conditions. When management uses its social influence within the organization to underscore the

importance of reviewing and rehearsing plans, it communicates the value and expectation of such behaviors.

Participants A2 and A3 underscored the importance of maintaining a dynamic BCP that is subject to ongoing review and continuous enhancement. Regular training is essential for the team's development and for enhancing their ability to respond effectively in the event of disasters. Both viewpoints highlight that incremental improvements are crucial to organizational resilience, even when perfection is not expected. Furthermore, A2 emphasized the necessity of robust DRP and BCP planning, particularly in terms of establishing redundancies, conducting rigorous testing, and the importance of clear and effective communication. These elements collectively enable teams to respond more efficiently to potential cyber-attacks and other disruptive incidents. These elements would not be met if DRP and BCP remain static; therefore, dynamic and continuous review and enhancement are necessary to face ongoing cybersecurity challenges.

These approaches are consistent with the perspective of Kesa (2023), who supports the need for continual improvement and regular assessment of information technology DRP and BCP practices. Furthermore, the evolving BCP and DRP routine addresses performance expectancy by enhancing team performance in response to a cybersecurity breach, while also acknowledging the effort required to execute the plans, valuing progress over unattainable perfection, which aligns with effort expectancy. Furthermore, a strong technical and procedural system supports the staff's ability to respond to an attack, which in turn facilitates conditions. All these elements are done to

improve the adoption and sustained utilization of recent technologies and systems, such as a living, regularly updated business continuity plan.

Participant A4 contributes to the perspective by emphasizing the critical role of employee training and simulation exercises in enhancing an organization's preparedness for cyberattacks and other disruptive events. Emphasizing training and practice enables teams to respond more efficiently, which ensures comprehension and execution can occur under pressure. Regular participation in simulations helps staff internalize response protocols, which increases confidence and capability during actual incidents. This approach aligns with Kesa (2023), who advocates ongoing improvement and frequent evaluation of disaster recovery and business continuity practices.

Continuous training and simulation foster technical competence and adaptive learning, allowing teams to refine their response strategies over time. When employees witness tangible improvements in team responsiveness and recovery outcomes, their confidence in the plan increases. Furthermore, valuing progress and incremental enhancement over unattainable perfection exemplifies effort expectancy, as it reduces the pressure on staff and makes plan adoption more manageable. Supporting these processes with robust technical and procedural systems demonstrates the importance of creating facilitating conditions, ensuring that employees have the necessary resources, infrastructure, and guidance for the successful execution of recovery plans.

Implementation Constraints

While emphasizing the importance of maintaining multiple redundant systems and performing regular tests is important, Participant A2 noted that many organizations

often prioritize efficiency and productivity, which can limit the opportunity for ongoing testing. A2 suggests streamlining disaster recovery plans by reducing the number of participants, clarifying roles, and promoting greater business involvement in planning to address excessive personnel and decision-making confusion during cyber incidents. Bhakuni and Saxena (2023) highlighted critical human resource challenges, including sustaining skilled personnel and implementing robust employee training without disrupting normal operations. Additionally, Hugelius et al. (2020) emphasized the need to establish effective crisis management structures and team coordination, while striking a balance between contingency planning and real-time operational needs. When it comes to the acceptance of DRP and BCP, there is a need to demonstrate tangible benefits (performance expectancy), minimize procedural complexity (effort expectancy), foster strong leadership and peer support (social influence), and ensure sufficient resources and training (facilitating conditions). Addressing these dimensions can strengthen acceptance, engagement, and consistency for DRP and BCP, thereby enhancing organizational resilience.

A3 and A4 noted that companies that have not previously experienced a cyber-attack often consider themselves to be at lower risk. This perception can result in these organizations making fewer investments in DRP and BCP initiatives. A4 underscored the complexity of coordinating various roles within an organization's DRP and BC processes. They emphasized that assigning too many responsibilities to one individual can lead to overload and inefficiency. Conversely, designating a single person for each discrete task may result in fragmentation and a lack of cohesion. This delicate balance

makes team selection and role assignment a challenging process, which requires careful consideration to ensure both effectiveness and manageability within the organization. Kesa (2023) identified increasing complexity of technology, ongoing budgetary limitations, internal organizational resistance to change, and the persistent need for skilled personnel as significant challenges that organizations commonly encounter when implementing DRP and BCP strategies. These challenges become more significant among those who underestimate their risk due to a lack of prior incidents. These challenges focus on the social influence and facilitating conditions portion of adoption, which can help explain the lower adoption despite the need for DRP and BCP strategies. Social influence is evident in their tendency to downplay risk in the absence of previous cyber-attacks, which can lead to insufficient investment in critical DRP and BC activities, thereby lowering the facilitating conditions as well.

Despite the literature review highlighting the need for DRP and BCP, certain attitudes reveal hesitation toward implementation. A1 addressed these perceptions by emphasizing the necessity of transparency in communicating strategic plans and substantiating their effectiveness. This method helps integrate cyber safety into the organizational culture, ensuring that employees understand the implications of cyber-attacks and their role in prevention. Tolossa (2023) argues that mitigating negative attitudes requires comprehensive cybersecurity awareness training, positioning employees as the first line of defense and fostering an environment that is mindful of cybersecurity practices. Additionally, research indicates that human behavior frequently presents the most significant vulnerability in cyber threat prevention, underscoring the

vital importance of robust staff training (Quader & Janeja, 2021). Therefore, transparency helps convert negative attitudes into positive ones for implementing DRP and BCP.

These strategies align with social influence because attitudes can jeopardize the adoption of technology.

A4 described a targeted approach for maintaining the effectiveness of DRP while minimizing their impact on job performance, which can affect attitudes toward DRP and BCP. They achieved this balance by scheduling regular, concise 30-minute meetings with employees to reinforce each team member's sense of organizational value and ensure a clear understanding of their specific responsibilities within the broader DRP. This method helps foster a supportive environment and encourages active participation in continuity planning. Benqdara (2024) identified widespread issues regarding employee awareness and compliance in information security, as well as non-compliance attitudes. These often resulted in a lack of awareness or a deliberate choice to disregard, both of which could lead to a data breach. Both can reflect an attitude toward DRP and BCP, which makes the strategies necessary to improve awareness and reduce the likelihood that employees will disregard them. Benqdara noted that comprehensive communication and educational initiatives are effective mitigation strategies for negative attitudes toward security policy. To address these challenges, comprehensive communication and educational initiatives are recommended as effective mitigation strategies. By routinely engaging employees and clarifying their roles, organizations can better promote adherence to established security protocols.

Information Technology Contributions and Recommendations for Professional Practice

The findings of this study offer valuable insights for organizations seeking to establish effective DRP and BCP strategies. Initially, DRP and BCP should be integrated into the cybersecurity process, as they are crucial for maintaining operations during and after a cyber incident. Integrating them strengthens resilience by ensuring that critical systems and data can be restored, and essential functions can continue, thereby minimizing downtime and financial loss. BCP will ensure that critical business functions can continue operating during and after a cyber-attack. Its purpose is to keep the business running, even at a reduced capacity. For example, a BCP might ensure essential systems remain accessible while a more extensive recovery is underway, a process that also requires strong cybersecurity to prevent reinfection. A DRP will focus on restoring IT systems and data after a disruptive event, such as a cyberattack. Its purpose is to bring the IT infrastructure and data back to a functional state. For example, a DRP would include steps to recover lost or corrupted data from a ransomware attack without reinfecting the restored systems, which all four participants provided consistent input leading to this statement.

Companies that proactively work to maintain operations following a cyberattack can leverage these results to strengthen their plans. The data analysis revealed that all managers adhere to established policies and regulatory processes when implementing recovery measures. Additionally, it was noted that managers often employ individualized methods that are not part of standard procedures during the implementation phase. For IT

organizations, it is crucial to continuously update their strategies for addressing insider threats. Staying current with emerging risks and approaches allows organizations to respond effectively to internal security challenges. Security practitioners can benefit from conducting regular internal process inspections within their area of responsibility. These inspections facilitate the identification of gaps in existing approaches. While the participants may have provided varying details, each of them conveyed the same core message related to the above. The study highlights that such gaps may be addressed by adopting the implementation practices identified in the research, thereby enhancing the organization's overall security posture.

Implications for Social Change

The implications of this study's findings for positive social change and the strategies applied may offer senior security managers opportunities to improve their customers' confidence in their employed practices. By incorporating the findings of this study within the company's DRP and BCP strategy, a robust framework can be documented for customer feedback. This level of openness regarding security posturing can instill confidence in the populace about the respect an organization shows when handling personal information. This led to another implication for social change, namely the sense of security that an organization's customers experience when personally identifiable information is used during online transactions.

Since the beginning of this study, numerous data breaches have occurred, exposing customers' personally identifiable information to unknown entities. Recent significant cyber-attacks include the May 2024 ransomware attack on Change Healthcare,

the September 2025 attack on Jaguar Land Rover and other UK retailers, and the August 2025 attacks on Italian hotels, Workday, Bragg Gaming Group, and Allianz Life Insurance Company. These attacks employed various tactics, including ransomware, data theft, and exploitation of supply chain vulnerabilities (Major Cyber Attacks, 2025). From a consumer perspective, they do not care how or why; they want their personal information to be secure and readily available when needed. A DRP and BCP could help in this case.

The findings detailed in this study make a significant contribution to the existing body of knowledge available in peer-reviewed resources on disaster recovery and business continuity. By examining real-world examples, the study sheds light on previously unknown steps organizations can take to enhance their security measures. These practical insights provide security professionals with new strategies beyond those learned from past experiences or educational institutions, which may not be sufficient for strengthening internal capabilities.

Further implications for social change arising from this study include the importance of promoting efforts to secure the personal information of global customers. The distinction of global customers is that they reflect different cultural values and levels of internet experience, which in turn lead to varying expectations of privacy regarding consumer information (Bellman et al., 2004). Gupta et al. (2016) demonstrated that global customers do not share a uniform approach by illustrating how Indian consumers are generally more willing to share sensitive personal data. In contrast, U.S. customers tend to adopt more measures to safeguard their privacy. Zhang et al. (2002) further

emphasized that privacy concerns are closely tied to differing social and economic contexts, which often result in global e-commerce platforms developing localized strategies to address the varied privacy expectations and requirements. While challenging, it is essential to maintain these different expectations with DRP and BCP within the global market to ensure that global customers are not vulnerable to identity theft-related attacks.

This is particularly crucial for shaping social perceptions, mainly as organizations increasingly collect and store personal data for analytical purposes. In such scenarios, users' information is exposed to a heightened risk of data theft, underscoring the need for robust security measures. The study highlights that securing personal digital information has become a growing concern for IT companies over the past several decades. Collegiate institutions are encouraged to incorporate updated strategies identified in this study into their curricula. By doing so, they can enhance lessons and training focused on insider threat mitigation, thereby equipping future professionals with the tools necessary to improve security practices within organizations.

Recommendations for Further Research

This study has highlighted several strategies utilized by IT managers and cybersecurity leaders in DRP and BCP following cyberattacks. The research focused on identifying specific implementation strategies that IT managers in the United States employed to maintain production with minimal downtime after such incidents.

One major limitation encountered was a lack of cooperation from IT leaders. Many were hesitant to disclose their operational methods, even after being assured that

the research centered on their individual experiences rather than company protocols. Companies must recognize that successful DRP and BCP implementation requires adequate training and inevitably leads to some loss of productive time. While the scope of this study was limited to the United States, expanding the research to include DRP and BCP practices in other countries could further validate the findings and confirm their applicability across different sectors. Replicating this study in various international contexts would help authenticate participants' perspectives and ascertain the broader relevance of the identified strategies.

Another limitation involved the challenge of obtaining a sufficiently large sample size to answer the central research question. Data saturation was achieved after conducting four interviews, with recurring themes and findings among all participants. Triangulation was employed by cross-referencing interview data with member checking sessions and by comparing emerging themes with industry documentation. Employing a quantitative research design could facilitate the recruitment of more participants, thereby increasing the sample size. Future research should consider evaluating the main research question using alternative research designs to compare results and further strengthen the study's conclusions.

A third limitation was the variation in participants' experience levels. The study included IT managers with at least ten years of experience in cloud computing technology and in implementing DRP and BCP within the United States. These participants had experience working in multiple information technology companies in the Southeast United States and had managed teams of three or more members. However, the

study did not include chief information officers, chief information security officers, chief technology officers, IT presidents, or vice presidents, who also play significant roles in implementing cybersecurity strategies. Including these positions in future research could help identify additional strategies for implementing DRP and BCP after cyber-attacks.

Conclusions

Information technology leaders and managers should prioritize revising existing security programs and strategies, focusing on security management practices, protective technology tools, and ongoing training to enhance overall security. Robust security policies and procedures, combined with strategic planning, training, and user awareness, are essential for managing the effective transition of DRP and BCP after a cyber-attack. The findings of this study highlight several key strategies that IT leaders employ to safeguard information systems after a cyberattack. Firstly, it is vital to accurately identify the event and assess its impact, including determining affected systems and channels, and swiftly isolating the attack. Secondly, alternative delivery approaches, such as shifting operations to another region or data center, can help sustain business continuity during containment and solution development. Thirdly, implementing concentric circles of protection for data and systems is important to guard against potential failures and disasters. Finally, conducting semi-annual reviews of DRP and BCP plans and practicing their execution using real-world scenarios are necessary steps for maintaining readiness and resilience.

References

- Abid, S.K., Sulaiman, N.B., Chan, S.W., Nazir, U., Abid, M., Han, H., Ariza-Montes, A., & Vega-Muñoz, A. (2021). Toward an integrated disaster management approach: How artificial intelligence can boost disaster management. *Sustainability*.
<https://doi.org/10.3390/su132212560>
- Abrahams, T. O., Farayola, O. A., Amoo, O. O., Ayinla, B. S., Osasona, F., & Atadoga, A. (2024). Continuous improvement in information security: A review of lessons from superannuation cybersecurity programs. *International Journal of Science and Research Archive*, 11(1), 1327–1337.
<https://doi.org/10.30574/ijrsra.2024.11.1.0219>
- Abualkishik, A. Z., A., A., & Gulzar, Y. (2020). Disaster recovery in cloud computing systems: An overview. *International Journal of Advanced Computer Science and Applications*, 11(9). <https://doi.org/10.14569/ijacsa.2020.0110984>
- Adekunle, S. A., Aigbavboa, C., Ejohwomu, O., Ikuabe, M., & Ogunbayo, B. (2022, June 20). *A critical review of maturity model development in the digitisation era*. MDPI. <https://doi.org/10.3390/buildings12060858>
- Adenekan, O. A., Ezeigweneme, C., & Chukwurah, E. G. (2024). Strategies for protecting it supply chains against cybersecurity threats. *International Journal of Management & Entrepreneurship Research*, 6(5), 1598–1606.
<https://doi.org/10.51594/ijmer.v6i5.1125>
- Ahmed, M. S., Everatt, J., Fox-Turnbull, W., & Alkhezzi, F. (2023). Systematic review of literature for smartphones technology acceptance using unified theory of

- acceptance and use of technology model (UTAUT). *Social Networking*, 12(02), 29–44. <https://doi.org/10.4236/sn.2023.122002>
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-t](https://doi.org/10.1016/0749-5978(91)90020-t)
- Alabdullah, J. H., Van Lunen, B. L., Claiborne, D. M., Daniel, S. J., Yen, C., & Gustin, T. S. (2020). Application of the unified theory of acceptance and use of technology model to predict dental students' behavioral intention to use tele dentistry. *Journal of Dental Education*, 84(11), 1262–1269. <https://doi.org/10.1002/jdd.12304>
- Alnoukari, M. (2021). From business intelligence to big data: The power of analytics. In A. Azevedo & M. Santos (Eds.), *Integration Challenges for Analytics, Business Intelligence, and Data Mining* (pp. 44-62). IGI Global Scientific Publishing. <https://doi.org/10.4018/978-1-7998-5781-5.ch003>
- Alshahrani, A., Stewart, D., & MacLure, K. (2019). A systematic review of the adoption and acceptance of eHealth in Saudi Arabia: Views of multiple stakeholders. *International Journal of Medical Informatics*, 128, 7-17. <https://doi.org/10.1016/j.ijmedinf.2019.05.007>
- Alomoto, W., Niñerola, A., & Pié, L. (2021). Social impact assessment: A systematic review of literature. *Social Indicators Research*, 161(1), 225–250. <https://doi.org/10.1007/s11205-021-02809-1>
- Amajuoyi, C.P., Nwobodo, L.K. & Adegbola, M.D. (2024). Transforming business

scalability and operational flexibility with advanced cloud computing technologies. *Computer Science & IT Research Journal*. 5. 1469-1487.

<https://doi.org/10.51594/csitj.v5i6.1248>.

Angafor, G. N., Yevseyeva, I., & Maglaras, L. (2023). Scenario-based incident response training: Lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. *Information & Computer Security*, 31(4), 404–426. <https://doi.org/10.1108/ics-05-2022-0085>

Anufriyeva, V., Pavlova, M., Stepurko, T., & Groot, W. (2020). The validity and reliability of self-reported satisfaction with healthcare as a measure of quality: a systematic literature review. *International journal for quality in health care : journal of the International Society for Quality in Health Care*.

<https://doi.org/10.1093/intqhc/mzaa152>

Apurva, P., Kermanshachi, S., & Sanjgna, K. (2020). Impact of natural disasters on construction projects: Strategies to prevent cost and schedule overruns in reconstruction projects. <https://doi.org/10.3311/cc2020-054>

Artykutsa, S., & Prokhorova, A. (2021). Features of qualitative interviews with injection drug users. *NaUKMA Research Papers. Sociology*, 4, 73–80.

<https://doi.org/10.18523/2617-9067.2021.4.73-80>

Ayaz, A., & Yanartas, M. (2020). An analysis on the unified theory of acceptance and use of technology theory (UTAUT): Acceptance of electronic document management system (EDMS). *Computers in Human Behavior Reports*, 2, 100032.

<https://doi.org/10.1016/j.chbr.2020.100032>

- Ayeni, A. J. (2020). Teachers' Capacity Building and Productivity in Secondary Schools in Ondo North Senatorial District of Ondo State, Nigeria. *Innovative Studies: International Journal (ISIJ)*, 3, 1-9
<https://www.cscjournals.org/manuscript/Journals/ISIJ/Volume3/Issue1/ISIJ-31.pdf>
- Baizat, F., Rahma, Z., & Abusaid, S. (2022). The dark side of IT: The negative aspects of information technology. *International Journal of Technology and Systems*, 7(2), 95–115. <https://doi.org/10.47604/ijts.1709>
- Bhakuni, S., & Saxena, S. (2023). Exploring the link between training and development, employee engagement, and employee retention. *Journal of Business and Management Studies*, 5(1), 173–180. <https://doi.org/10.32996/jbms.2023.5.1.17>
- Bhuvana, R., & Aithal, P. S. (2022). Investors behavioral intention of cryptocurrency adoption – A review based research agenda. *International Journal of Applied Engineering and Management Letters*, 126–148.
<https://doi.org/10.47992/ijaeml.2581.7000.0125>
- Boland, J., Banks, S., Krabbe, R., Lawrence, S., Murray, T., Henning, T., & Vandenberg (2022). A COVID-19-era rapid review: using Zoom and Skype for qualitative group research. *Public health research & practice*, 32 2.
<https://doi.org/10.17061/phrp31232112>
- Bull, S., & Bhagwandin, N. (2020). The ethics of data sharing and Biobanking in health research. *Wellcome Open Research*, 5, 270.
<https://doi.org/10.12688/wellcomeopenres.16351.1>

- Butera, F., Batruch, A., Autin, F., Mugny, G., Quiamzade, A., & Pulfrey, C. (2020). Teaching as social influence: Empowering teachers to become agents of Social Change. *Social Issues and Policy Review*, *15*(1), 323–355.
<https://doi.org/10.1111/sipr.12072>
- Campbell, K., Orr, E., Durepos, P., Nguyen, L., Li, L., Whitmore, C., Gehrke, P., Graham, L., & Jack, S. (2021). Reflexive thematic analysis for applied qualitative health research. *The Qualitative Report*. <https://doi.org/10.46743/2160-3715/2021.5010>
- Capps, J. (2023, May 22). *The pragmatic theory of truth*. Stanford Encyclopedia of Philosophy. <https://plato.stanford.edu/archives/sum2023/entries/truth-pragmatic/>
- Casteel, A., & Bridier, N. (2021). Describing populations and samples in doctoral student research. *International Journal of Doctoral Studies*, *16*, 339–362.
<https://doi.org/10.28945/4766>
- Cernasev, A., & Axon, D.R. (2023). Research and scholarly methods: Thematic analysis. *Journal of the American College of Clinical Pharmacy*, *6*, 751 - 755.
<https://doi.org/10.1002/jac5.1817>
- Chai, H. H., Gao, S. S., Chen, K. J., Duangthip, D., Lo, E. C., & Chu, C. H. (2021). A concise review on qualitative research in dentistry. *International Journal of Environmental Research and Public Health*, *18*(3), 942.
<https://doi.org/10.3390/ijerph18030942>
- Charoenthammacheke, K., Leelawat, N., Tang, J., & Kodaka, A. (2020). Business continuity management: A preliminary systematic literature review based on

ScienceDirect database. *Journal of Disaster Research*.

<https://doi.org/10.20965/jdr.2020.p0546>

Chen, J.-H., Ha, N. T., Tai, H.-W., & Chang, C.-A. (2020). The willingness to adopt the internet of things (IOT) conception in Taiwan's construction industry. *Journal of Civil Engineering and Management*, 26(6), 534–550.

<https://doi.org/10.3846/jcem.2020.12639>

Chen, L., Tong, T.W., Tang, S., & Han, N. (2021). Governance and design of digital platforms: A review and future research directions on a meta-organization. *Journal of Management*, 48, 147 - 184.

<https://doi.org/10.1177/01492063211045023>

Chi, T. W., & Mahmud, I. (2020). Business intelligence system adoption: A systematic literature review of two decades. *International Journal of Industrial Management*, 6, 1–8. <https://doi.org/10.15282/ijim.6.0.2020.5624>

Christou, P. A. (2022). How to use thematic analysis in qualitative research. *Journal of Qualitative Research in Tourism*, 3(2), 79–95.

<https://doi.org/10.4337/jqrt.2023.0006>

Chroustová, K., Šorgo, A., Bílek, M., & Rusek, M. (2022). Differences in chemistry teachers' acceptance of educational software according to their user type: An application of extended UTAUT model. *Journal of Baltic Science Education*, 21(5), 762–787. <https://doi.org/10.33225/jbse/22.21.762>

Chung, A., Vieira, D., Donley, T., Tan, N., Jean-Louis, G., Kiely Gouley, K., & Seixas, A. (2021). Adolescent peer influence on eating behaviors via social media:

Scoping review. *Journal of Medical Internet Research*, 23(6).

<https://doi.org/10.2196/19697>

Chung, C. J., Biddix, J. P., & Park, H. W. (2020). Using digital technology to address confirmability and scalability in thematic analysis of participant-provided data.

The Qualitative Report. <https://doi.org/10.46743/2160-3715/2020.4046>

Connolly, M. J., Weppner, W. G., Fortuna, R. J., & Snyder, E. D. (2022). Continuity and health outcomes in resident clinics: A scoping review of the literature. *Cureus*.

<https://doi.org/10.7759/cureus.25167>

Corrales-Estrada, A.M., Gómez-Santos, L., Bernal-Torres, C.A., & Rodríguez-López, J.E. (2021). Sustainability and resilience organizational capabilities to enhance business continuity management: A literature review. *Sustainability*.

<https://doi.org/10.3390/su13158196>

Cox, S., Solbakk, J. H., & Bernabe, R. D. (2021). The role of research ethics committees after the approval of clinical trial protocols in the EU and the USA: A descriptive content analysis of international and regional normative documents. *Current Medical Research and Opinion*, 37(6), 1061–1069.

<https://doi.org/10.1080/03007995.2021.1905621>

Dang, L., & Weiss, J. (2021). Evidence on the relationship between place attachment and behavioral intentions between 2010 and 2021: A systematic literature review.

Sustainability, 13(23), 13138. <https://doi.org/10.3390/su132313138>

Darmansyah, R., Handoko, T., & Tiyas Tinov, M. Y. (2020). Review of the provision of employee management information system at the Pekanbaru City Personnel and

Human Resources Development Agency in supporting the e-government policy in 2019. *Journal of Political and Social Administration*, 1(1), 19–33.

<https://doi.org/10.46730/japs.v1i1.8>

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of Information Technology. *MIS Quarterly*, 13(3), 319.

<https://doi.org/10.2307/249008>

Denny, E., & Weckesser, A. (2022). Quality not quantity. *BJOG: An International Journal of Obstetrics & Gynaecology*, 129(10), 1799–1800.

<https://doi.org/10.1111/1471-0528.17149>

Dewey, D. (2024). Is limitation of liability an illusion? Examining the numbers and current trends of the Limitation Act Today. *Loyola Maritime Law Journal*, 23(2).

<https://loyolamaritimelawjournal.scholasticahq.com/article/117703-is-limitation-of-liability-an-illusion-examining-the-numbers-and-current-trends-of-the-limitation-act-today>

Dewi, E. A., Sanofi, Z., Pratamawaty, B. B., & Arifin, H. S. (2023). Implementation of the unified theory of acceptance and use of technology (utaut) model during the pandemic era: A systematic literature review (SLR). *Jurnal Komunikasi: Malaysian Journal of Communication*, 39(3), 313–350.

<https://doi.org/10.17576/jkmjc-2023-3903-17>

Do, H. J., Kong, H.-K., Tetali, P., Karahalios, K., & Bailey, B. P. (2023). Inform, explain, or control: Techniques to adjust end-user performance expectations for a conversational agent facilitating group chat discussions. *Proceedings of the ACM*

on *Human-Computer Interaction*, 7(CSCW2), 1–26.

<https://doi.org/10.1145/3610192>

Dougherty, M. V. (2021). The use of confidentiality and anonymity protections as a cover for fraudulent fieldwork data. *Research Ethics*, 17, 480 - 500.

<https://doi.org/10.1177/17470161211018257>

Dwivedi, Y. K., Rana, N. P., Tamilmani, K., & Raman, R. (2020). A meta-analysis based modified unified theory of acceptance and use of Technology (meta-utaut): A Review of Emerging Literature. *Current Opinion in Psychology*, 36, 13–18.

<https://doi.org/10.1016/j.copsyc.2020.03.008>

Elias, P. (2024). Research methods: qualitative observation. *Wounds UK*, 20(1).

<https://wounds-uk.com/journal-articles/research-methods-qualitative-observation/>

Facca, D., Smith, M. J., Shelley, J., Lizotte, D., & Donelle, L. (2020). Exploring the ethical issues in research using digital data collection strategies with minors: A scoping review. *PLOS ONE*, 15(8). <https://doi.org/10.1371/journal.pone.0237875>

Fauzi, R., & Lubis, M. (2021). Assessment framework for defining the maturity of information technology within enterprise risk management (ERM). *International Journal of Advanced Computer Science and Applications*, 12(10).

<https://doi.org/10.14569/ijacsa.2021.0121075>

Finucane, M. L., Acosta, J., Wicker, A., & Whipkey, K. (2020). Short-term solutions to a long-term challenge: Rethinking disaster recovery planning to reduce vulnerabilities and inequities. *International Journal of Environmental Research and Public Health*, 17(2), 482. <https://doi.org/10.3390/ijerph17020482>

- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Addison-Wesley.
- Frye, S., Butterfield, R., & Hoffman, J. M. (2021). SNMMI Clinical Trials Network Research Series for Technologists: Ethical issues and regulations in the medical workplace. *Journal of Nuclear Medicine Technology*, 49(4), 303–310.
<https://doi.org/10.2967/jnmt.121.263100>
- Fuchs, K. (2023). A systematic guide for conducting thematic analysis in qualitative tourism research. *Journal of Environmental Management and Tourism*, 14(6), 2696. [https://doi.org/10.14505/jemt.v14.6\(70\).17](https://doi.org/10.14505/jemt.v14.6(70).17)
- Fusch, P., & Ness, L. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, 20(9), 1408–1416. <https://doi.org/10.46743/2160-3715/2015.2281>
- Gallegos, D., Durham, J., Rutter, C., & McKechnie, R. (2023). Working towards the Active Participation of Underrepresented Populations in Research: A Scoping Review and Thematic Synthesis. *Health & Social Care in the Community*.
<https://doi.org/10.1155/2023/1312525>
- Ganesen, R., Bakar, A. A., Ramli, R., Rahim, F. A., & Zawawi, M. N. (2022). Cybersecurity risk assessment: Modeling factors associated with higher education institutions. *International Journal of Advanced Computer Science and Applications*, 13(8). <https://doi.org/10.14569/ijacsa.2022.0130843>
- Gatzioufa, P., & Saprikis, V. (2022). A literature review on users' behavioral intention toward Chatbots' adoption. *Applied Computing and Informatics*.

<https://doi.org/10.1108/ACI-01-2022-0021>

Ghimire, N. B. (2021). Review on ethical issues in ethnographic study: Some reflections.

Contemporary Research: An Interdisciplinary Academic Journal, 5(1), 79–94.

<https://doi.org/10.3126/craiaj.v5i1.40485>

Gnanapragasam S. N., Hariman K, Ventriglio A. (2021). Editorial: To Zoom or not to

Zoom – that is the question. *International Journal of Social Psychiatry*;67(8):974-

976. <https://doi.org/10.1177/00207640211004991>

Green, C. (2023). Best practices in supplier relationship management and response when

supply is disrupted by cyber Attack : An incident response framework. *Journal of*

Business Continuity & Emergency Planning, 17(1), 6.

<https://doi.org/10.69554/grlb2974>

Grod, I., Balyk, N., Vasylenko, Y., Martyniuk, S., Oleksiuk, V., & Barna, O. (2022).

Web service of works planning using network graph. *Physical and Mathematical*

Education, 34(2), 18–24. <https://doi.org/10.31110/2413-1571-2022-034-2-003>

Gunawan, I., Redi, A. A., Santosa, A. A., Maghfiroh, M. F., Pandyaswargo, A. H., &

Kurniawan, A. C. (2022). Determinants of customer intentions to use electric

vehicle in Indonesia: An integrated model analysis. *Sustainability*, 14(4), 1972.

<https://doi.org/10.3390/su14041972>

Habibi Rad, M., Mojtahedi, M., & Ostwald, M.J. (2021). The Integration of lean and

resilience paradigms: A systematic review identifying current and future research

directions. *Sustainability*. <https://doi.org/10.3390/su13168893>

Hashim, R., Bakar, A., Noh, I., & Mahyudin, H.A. (2020). Employees' Job satisfaction

and performance through working from home during the pandemic lockdown.

Environment-Behaviour Proceedings Journal.

<https://doi.org/10.21834/ebpj.v5i15.2515>

Hempenius, N., Chou, T. S., & Toderick, L. (2021). Challenges of virtual machine performance in information and computer technology virtual lab environments. In *Proceedings of the 2020 Conference for Industry and Education Collaboration, CIEC 2020*. American Society for Engineering Education.

<https://doi.org/10.18260/1-2-00-38719>

Hessels, R. S., & Hooge, I.T. (2021). Dogmatic modes of science. *Perception*, 50, 913 -

916. <https://doi.org/10.1177/03010066211047826>

Higashi, A. K., Mazuco, F. C., Santos, H. M., & Flores, D. (2020). Trusted digital environments for holistic archival document preservation. *Information &*

Information, 25(4), 499. <https://doi.org/10.5433/1981-8920.2020v25n4p499>

Hodge, J., Foley, S., Brankaert, R., Kenning, G., Lazar, A., Boger, J., & Morrissey, K.

(2020). Relational, flexible, everyday: Learning from ethics in dementia research.

Proceedings of the 2020 CHI Conference on Human Factors in Computing

Systems, 1–16. <https://doi.org/10.1145/3313831.3376627>

Holovnia, O. S., Shchur, N. O., Sverchevska, I. A., Bailiuk, Y. M., & Pokotylo, O. A.

(2023). Interactive surveys during online lectures for it students. *CTE Workshop*

Proceedings, 10, 185–206. <https://doi.org/10.55056/cte.556>

Houtkin, A. (2024). Aligning disaster recovery to company technical direction and

objectives. *Journal of Business Continuity & Emergency Planning*, 17(3),

206. <https://doi.org/10.69554/pyaf3904>

- Huapaya-Ruiz, R., & Meneses-Claudio, B. (2024). Applicable methodologies for business continuity management in IT services: A systematic literature review. *Data and Metadata*. <https://doi.org/10.56294/dm202418>
- Hugelius, K., Becker, J., & Adolfsson, A. (2020). Five challenges when managing mass casualty or disaster situations: A Review Study. *International Journal of Environmental Research and Public Health*, 17. <https://doi.org/10.3390/ijerph17093068>
- Hussain, M. I., Figueiredo, M. C., Tran, B. D., Su, Z., Molldrem, S., Eikey, E. V., & Chen, Y. (2020). A scoping review of qualitative research in Jamia: Past contributions and opportunities for future work. *Journal of the American Medical Informatics Association*, 28(2), 402–413. <https://doi.org/10.1093/jamia/ocaa179>
- Ibrahim, O. (2024). Impact of cloud computing on business continuity and disaster recovery. *Journal of Technology and Systems*. 6. 16-28. 10.47941/jts.2146. <https://doi.org/10.47941/jts.2146>
- Irawan, I. (2023). Development of resource management and performance management in improving the quality function of human resources: A literature review. *BRILLIANT: Journal of Management and Business Economics*, 3(2), 215–228. <https://doi.org/10.55606/cemerlang.v3i2.1174>
- Irkey, T., & Tüfekci, A. (2021). The importance of business continuity and knowledge management during the pandemic period. *The 7th International Management Information Systems Conference*, 15, 18.

<https://doi.org/10.3390/proceedings2021074018>

Jerez, O., Orsini, C., Ortiz, C., & Hasbun, B. (2021). Which conditions facilitate the effectiveness of large group learning activities? A systematic review of research in Higher Education. *Learning: Research and Practice*, 7(2), 147–164.

<https://doi.org/10.1080/23735082.2020.1871062>

Kakar, Z. U., Rasheed, R., Rashid, A., & Akhter, S. (2023). Criteria for assessing and ensuring the trustworthiness in qualitative research. *International Journal of Business Reflections*, 4(2), 150–173. <https://doi.org/10.56249/ijbr.03.01.44>

Kamal, M., & Subriadi, A. P. (2021). UTAUT model of mobile application: Literature review. *2021 International Conference on Electrical and Information Technology (IEIT)*, 120–125. <https://doi.org/10.1109/ieit53149.2021.9587377>

Kamarudin, H. D., Jamaluddin, A., & Samsuddin, A. Z. (2024). Enhancing business continuity plans and records management in Selangor smes. *GATR Global Journal of Business Social Sciences Review*, 12(1), 15–24.

[https://doi.org/10.35609/gjbssr.2024.12.1\(2\)](https://doi.org/10.35609/gjbssr.2024.12.1(2))

Kartashov, A., & Globa, L. (2024). Towards seamless multi-cloud integration: Strategic approach. *Control, navigation and communication systems. Collection of scientific papers*, 4(78), 79–83. <https://doi.org/10.26906/sunz.2024.4.079>

Kasim, M.M. (2020). On the practical consideration of evaluators' credibility in evaluating relative importance of criteria for some real-Life multicriteria problems: An overview. <https://doi.org/10.5772/intechopen.92541>

Kawtar, I., Karim, D., & Salah, B. (2020). Impact of change in business alignment:

- Evaluation with CBITA tool. *International Journal of Advanced Computer Science and Applications*, 11(10). <https://doi.org/10.14569/ijacsa.2020.0111062>
- Kesa, D. M. (2023). Ensuring resilience: Integrating disaster recovery planning and business continuity for Sustainable Information Technology Operations. *World Journal of Advanced Research and Reviews*, 18(3), 970–992. <https://doi.org/10.30574/wjarr.2023.18.3.1166>
- Khan, I., Agarwal, N., Eeti, S., Goel, O., Jain, P.A., & Goel, P.P. (2024). Optimization techniques for 5G O-RAN deployment in cloud environments. *Darpan International Research Analysis*. <https://doi.org/10.36676/dira.v12.i3.135>
- Kleinheksel, A. J., Rockich-Winston, N., Tawfik, H., & Wyatt, T. R. (2020). Demystifying content analysis. *American Journal of Pharmaceutical Education*, 84(1), 7113. <https://doi.org/10.5688/ajpe7113>
- Kumar, S. (2023). Reviewing software testing models and optimization techniques: An analysis of efficiency and advancement needs. *Journal of Computers, Mechanical and Management*, 2(1), 32–46. <https://doi.org/10.57159/gadl.jcmm.2.1.23041>
- Laryeafio, M. N., & Ogbewe, O. C. (2023). Ethical consideration dilemma: Systematic review of ethics in qualitative data collection through interviews. *Journal of Ethics in Entrepreneurship and Technology*, 3(2), 94–110. <https://doi.org/10.1108/j eet-09-2022-0014>
- Li, X., & Li, R. (2024). A trustworthiness evaluation mechanism based on principles–assumptions model. *IEEE Internet of Things Journal*, 11(10), 17510–17524. <https://doi.org/10.1109/jiot.2024.3357705>

- Liang, M., Soomro, A., Tasneem, S., Abatti, L. E., Alizada, A., Yuan, X., Uusküla-Reimand, L., Antounians, L., Alvi, S. A., Paterson, A. D., Rivard, G.-É., Scott, I. C., Mitchell, J. A., Hayward, C. P. M., & Wilson, M. D. (2020, December 3). *Enhancer-gene rewiring in the pathogenesis of Quebec platelet disorder*. *Blood*. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7735161/>
- Linardos, V., Drakaki, M., Tzionas, P., & Karnavas, Y. L. (2022). Machine learning in disaster management: Recent developments in methods and applications. *Mach. Learn. Knowl. Extr.*, 4, 446-473. <https://doi.org/10.3390/make4020020>
- Lowe, S., Rod, M., Michel, H., & Hwang, K.-S. (2020). Towards a spectacularly dynamic and pluralist 'normal science': Pragmatism, communication, IMP, and BtoB marketing research. *Journal of Business & Industrial Marketing*, 35(11), 1739-1749. <https://doi.org/10.1108/JBIM-08-2019-0388>
- Luo, Y., Liu, W., Yue, X., & A. Rosen, M. (2020). Sustainable emergency management Based on intelligent information processing. *Sustainability*, 12, 1081. <https://doi.org/10.3390/su12031081>
- Mahapatra, I., Nagarajappa, R., Satyarup, D., & Mohanty, S. (2020). Considerations in Questionnaire Development: A Review. *Indian Journal of Forensic Medicine & Toxicology*. <https://doi.org/10.37506/ijfmt.v14i4.13054>
- Major cyber attacks, ransomware attacks, and data breaches: August 2025*. Home - Cyber Security Training. (2025, September 1). <https://www.cm-alliance.com/cybersecurity-blog/major-cyber-attacks-ransomware-attacks-and-data-breaches-august-2025>

- Mamidi, S. R. (2024). Securing multi-cloud architectures: A machine learning perspective. *Journal of Artificial Intelligence General science (JAIGS)* ISSN:3006-4023. <https://doi.org/10.60087/jaigs.v2i1.160>
- Mazimwe, A. ; Hammouda, I.; Gidudu, A. Implementation of FAIR principles for ontologies in the disaster. A systematic literature review. (2021) ISPRS Int. J. Geo-Inf. 2021, 10, 324. <https://doi.org/10.3390/ijgi10050324>
- Meechang, K., & Watanabe, K. (2022). The critical success factors of area-business continuity management: A systematic review and outlooks from the public and private sectors. *Journal of Disaster Research*, 17(6), 923–932. <https://doi.org/10.20965/jdr.2022.p0923>
- Megheirkouni, M., & Moir, J. (2023). Simple but effective criteria: Rethinking excellent qualitative research. *The Qualitative Report*. <https://doi.org/10.46743/2160-3715/2023.5845>
- Merseedi, K. J., & Zeebaree, D.S. (2024). Cloud architectures for distributed multi-cloud computing: A review of hybrid and federated cloud environment. *Indonesian Journal of Computer Science*. <https://doi.org/10.33022/ijcs.v13i2.3811>
- Mustafa, M., Alshare, M.I., Bhargava, D., Neware, R., Singh, B., & Ngulube, P. (2022). Perceived security risk based on moderating factors for blockchain technology applications in cloud storage to achieve secure healthcare systems. *Computational and Mathematical Methods in Medicine*, 2022. <https://doi.org/10.1155/2022/6112815>
- Naidu, P.R., Guruprasad, N., & Gowda, D. (2021). A high-availability and integrity layer

for cloud storage, cloud computing security: From single to multi-clouds. *Journal of Physics: Conference Series*, 1921. <https://doi.org/10.1088/1742-6596/1921/1/012072>

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research*. U.S. Department of Health and Human Services. <https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html>

Ngala, D. (2021). User involvement and performance of enterprise resource planning system implementation in multi-national organizations in Kenya. A case of Un-Habitat in Kenya. *Asian Journal of Research in Computer Science*, 49–63. <https://doi.org/10.9734/ajrcos/2021/v12i130276>

Ngenye, L., & Kreps, G. (2020). A review of qualitative methods in health communication research. *The Qualitative Report*, 25(3), 631-645. <https://doi.org/10.46743/2160-3715/2020.4488>

Ntshwarang, P.N., Malinga, T., & Losike-Sedimo, N. (2021). eLearning tools at the University of Botswana: Relevance and use under COVID-19 crisis. *Higher Education for the Future*, 8, 142 - 154. <https://doi.org/10.1177/2347631120986281>

Nyimbili, F., & Nyimbili, L. (2024). Types of purposive sampling techniques with their examples and application in qualitative research studies. *British Journal of Multidisciplinary and Advanced Studies*, 5(1), 90–99.

<https://doi.org/10.37745/bjmas.2022.0419>

Okoli, J. O. (2020). Improving decision-making effectiveness in crisis situations:

developing intuitive expertise at the workplace. *Development and Learning in Organizations*. <https://doi.org/10.1108/dlo-08-2020-0169>

Olorunyomi, T. D., Okeke, I.C., Sanyaolu, T.O., & Adeleke, A.G. (2024). Streamlining

budgeting and forecasting across multi-cloud environments with dynamic financial models. *Finance & Accounting Research Journal*.

<https://doi.org/10.51594/farj.v6i10.1643>

Ovrutsky, A. (2020). Information policy as communication concept. *Theoretical and*

Practical Issues of Journalism, 9(2), 307–324. [https://doi.org/10.17150/2308-6203.2020.9\(2\).307-324](https://doi.org/10.17150/2308-6203.2020.9(2).307-324)

Paraskevaidis, P. & Andriotis, K. (2023). Rethinking the evaluation criteria for

qualitative tourism research: introducing resynthesis. *Journal of Qualitative Research in Tourism*. 4. 36-51. <https://doi.org/10.4337/jqrt.2023.01.03>.

Pinto, D. C., Fernandes, A., da Silva, M.M., & Pereira, R. (2022). Maturity models for

business continuity—A systematic literature review. *International Journal of Safety and Security Engineering*. <https://doi.org/10.18280/ijssse.120115>

Pipera, M., & Fragouli, E. (2021). Employee well-being, employee performance &

positive mindset in a crisis. *The Business and Management Review*, 12(02).

<https://doi.org/10.24052/bmr/v12nu02/art-01>

Plaka, R. (2022). Backup & data recovery in cloud computing: A systematic mapping

study. *Ingenious*, 2(1), 94–113. <https://doi.org/10.58944/pwhk4843>

- Pollock NW. (2020). Managing bias in research. *Wilderness & Environmental Medicine*;31(1):1-2. <https://doi.org/10.1016/j.wem.2020.01.001>
- Pung, J., & Rienhoff, O. (2020). Key components and its assistance of participant management in clinical research: A scoping review. *JAMIA Open*, 3(3), 449–458. <https://doi.org/10.1093/jamiaopen/ooaa041>
- Putri, N. E., Helmi, H., Noer, M., & Yossyafra, Y. (2021). Systematic literature review (SLR) dinamika perencanaan pembangunan sustainable infrastructure. *Jurnal Public Policy*, 7(2), 103. <https://doi.org/10.35308/jpp.v7i2.3811>
- Raghavan, A., Demircioglu, M.A., & Orazgaliyev, S. (2021). COVID-19 and the new normal of organizations and employees: An overview. *Sustainability*.<https://doi.org/10.3390/su132111942>
- Ramakrishnan, R. (2022). Contingency planning to ensure business-as-usual. *International Journal of Progressive Sciences and Technologies*, 34(2), 476. <https://doi.org/10.52155/ijpsat.v34.2.4599>
- Reyes, M. (2020). Research in the time of COVID-19: Challenges of research ethics committees. *Journal of the ASEAN Federation of Endocrine Societies*, 35(1), 29–32. <https://doi.org/10.15605/jafes.035.01.07>
- Roberts, & Rosanne, E. (2020). Qualitative interview questions: Guidance for novice researchers. *The Qualitative Report*, 25, 3185-3203. <https://doi.org/10.46743/2160-3715/2020.4640>
- Rogers, E. M. (1995). *Diffusion of innovations*. The Free Press.
- Rouidi, M., Elouadi, A. E., Hamdoune, A., Choujtani, K., & Chati, A. (2022). TAM-

- UTAUT and the acceptance of remote healthcare technologies by healthcare professionals: A systematic review. *Informatics in Medicine Unlocked*, 32, 101008. <https://doi.org/10.1016/j.imu.2022.101008>
- Rowlands, J. (2021). Interviewee transcript review as a tool to improve data quality and participant confidence in sensitive research. *International Journal of Qualitative Methods*, 20, 160940692110661. <https://doi.org/10.1177/16094069211066170>
- Russo, N., Reis, L., Silveira, M. C., & Mamede, H.S. (2023). Towards a comprehensive framework for the multidisciplinary evaluation of organizational maturity on business continuity program management: A systematic literature Review. *Information Security Journal: A Global Perspective*, 33, 54 - 72. <https://doi.org/10.1080/19393555.2023.2195577>
- Saleem, M., Warsi, M. R., Islam, S., Anjum, A., & Siddiquii, N. (2021). Trust management in the world of cloud computing. Past trends and some new directions. *Scalable Comput. Pract. Exp.*, 22, 425-444. <https://doi.org/10.12694/scpe.v22i4.1952>
- Sapathai, S., Leelawat, N., Tang, J., Kodaka, A., Chintanapakdee, C., Ino, E., & Watanabe, K. (2020). A stakeholder analysis approach for area business continuity management: A systematic review. *Journal of disaster research*, 15, 588-598. <https://doi.org/10.20965/jdr.2020.p0588>
- Sarfaraz, MU., Hall, DM., and Rotman, RM. (2022) Data sharing in transboundary water management. *Front. Water* 4:982605. <https://doi.org/10.3389/fr.War.2022.982605>

- Sasaki, H., Maruya, H., Abe, Y., Fujita, M., Furukawa, H., Fuda, M., Kamei, T., Yaegashi, N., Tominaga, T., & Egawa, S. (2020). Scoping review of hospital business continuity plans to validate the improvement after the 2011 great East Japan earthquake and tsunami. *The Tohoku journal of experimental medicine*, 251(3), 147-159 . <https://doi.org/10.1620/tjem.251.147>
- Sammut, G., & Bauer, M. W. (2020). *The psychology of social influence: Modes and modalities of shifting common sense*. Cambridge University Press.
- Savita, & Verma. (2020). A review study on big data analysis Using R Studio. *International Journal of Engineering Technologies and Management Research*, 6(6), 129–136. <https://doi.org/10.29121/ijetmr.v6.i6.2019.402>
- Sharma, P., & Jha, A. (2024). The relevance of source credibility theory on purchase intention in the field the of marketing: A systematic literature review. *International Journal For Multidisciplinary Research*. <https://doi.org/10.36948/ijfmr.2024.v06i06.32130>
- Shatta, D. N. (2021). The influence of performance expectancy on e-procurement adoption model in developing countries: Tanzanians perception. *ITEGAM- Journal of Engineering and Technology for Industrial Applications (ITEGAM-JETIA)*. <https://doi.org/10.5935/jetia.v7i29.754>
- Shatta, D. N., & Mabina, B.K. (2024). The determinants of use behavior of e-procurement system in developing countries. *International Journal of Business Ecosystem & Strategy* (2687-2293). <https://doi.org/10.36096/ijbes.v6i2.498>
- Shaya, N., Madani, R., & Mohebi, L. (2023). An application and extension of the

- UTAUT model: Factors influencing behavioral intention to utilize mobile learning in UAE higher education. *Journal of Interactive Learning Research*, 34(1). <https://www.learntechlib.org/p/221534/>
- Shetty, R., Sharma, V., & Somesh, S. (2022). Review of disasters and recovery planning measures in IT sector. *International Journal of Scientific Research in Engineering and Management*, 06(08). <https://doi.org/10.55041/ijsrem16102>
- Shrivastava, S., Saini, G., & Agrawal, Y. (2023). Multi-cloud deployments and hybrid cloud architecture. Arya Institute of Engineering & Technology. <https://doi.org/10.48047/resmil.v10i1.16>
- Singh, A., Kaur, A., & Gupta, D. (2021). Reviewing trust issues in cloud computing. *Journal of Physics: Conference Series*, 1969(1), 012043. <https://doi.org/10.1088/1742-6596/1969/1/012043>
- Staddon, E., Loscri, V., & Mitton, N. (2021). Attack categorization for IOT applications in critical infrastructures, a survey. *Applied Sciences*, 11(16), 7228. <https://doi.org/10.3390/app11167228>
- Stahl, N. A., & King, J. R. (2020). *Expanding approaches for research: Understanding and using trustworthiness in qualitative research*. *Journal of Developmental Education*. <https://eric.ed.gov/?id=EJ1320570>
- Stamenkov, G. (2022). Layered business continuity and disaster recovery model. *Continuity & Resilience Review*, 4(3), 267–279. <https://doi.org/10.1108/crr-05-2022-0008>
- Stetsenko, V. V. (2021). Development and implementation of technologies for cultural

enlightenment in the context of state cultural policy: Semantic Guidelines and priority areas. *Communicology*, 9(2), 67–77. <https://doi.org/10.21453/2311-3065-2021-9-2-67-77>

Stevens, M. W. R., Delfabbro, P. H., & King, D. L. (2021). Prevention approaches to problem gaming: A large-scale qualitative investigation. *Computers in Human Behavior*, 115, 106611. <https://doi.org/10.1016/j.chb.2020.106611>

Suganya, M., & Sasipraba, T. (2021). An analysis of privacy preserving data storage and retrieval approaches in heterogeneous multi-cloud architectures. *Indian Journal of Computer Science and Engineering*.
<https://doi.org/10.21817/indjcse/2021/v12i4/211204074>

Sutrisno, Ausat, A. M., Permana, B., & Harahap, M. A. (2023). Do information technology and human resources create business performance: A review. *International Journal of Professional Business Review*, 8(8).
<https://doi.org/10.26668/businessreview/2023.v8i8.2206>

Szajna, A., & Kostrzewski, M. (2022). AR-AI tools as a response to high employee turnover and shortages in manufacturing during regular, pandemic, and war times. *Sustainability*. <https://doi.org/10.3390/su14116729>

Tabassum, N., Naeem, H., & Batool, A. (2023). The data security and multi-cloud privacy concerns. *International Journal for Electronic Crime Investigation*.
<https://doi.org/10.54692/ijeci.2023.0701128>

Tabesh, P., & Vera, D. (2020). Top managers' improvisational decision-making in crisis: A paradox perspective. *Management Decision*. <https://doi.org/10.1108/md-08->

[2020-1060](#)

- Taherdoost, H. (2022). What are different research approaches? Comprehensive review of qualitative, quantitative, and mixed method research, their applications, types, and limitations. *Journal of Management Science & Engineering Research*, 5(1), 53–63. <https://doi.org/10.30564/jmser.v5i1.4538>
- Tamilmani, K., Rana, N. P., Wamba, S. F., & Dwivedi, R. (2021). The extended unified theory of acceptance and use of technology (UTAUT2): A systematic literature review and theory evaluation. *International Journal of Information Management*, 57, 102269. <https://doi.org/10.1016/j.ijinfomgt.2020.102269>
- Tanwir, F., Moideen, S. Habib, R. (2021) Interviews in healthcare: A phenomenological approach to qualitative research methodology . *Journal of Public Health International* - 4(2):10-15. <https://doi.org/10.14302/issn.2641-4538.jphi-21-3881>
- Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, 6(2), 144–176. <https://doi.org/10.1287/isre.6.2.144>
- Thorne, S. E. (2016). *Interpretive description* (1st ed.). Routledge. <https://doi.org/10.4324/9781315426259>
- Thunberg, S., & Arnell, L. (2021): Pioneering the use of technologies in qualitative research – A research review of the use of digital interviews, *International Journal of Social Research Methodology*, <https://doi.org/10.1080/13645579.2021.1935565>
- Tolossa, D. (2023). Importance of cybersecurity awareness Training for employees in

business. *Vidya - A Journal of Gujarat University*, 2(2), 104–107.

<https://doi.org/10.47413/vidya.v2i2.206>

Tourish, D., & Craig, R. (2025). Is my research irresponsible? *Academy of Management Learning & Education*, 24(4), 497–511.

<https://doi.org/10.5465/amle.2024.0473>

Tuckerman, J., Kaufman, J., & Danchin, M. (2020). How to use qualitative methods for health and health services research. *Journal of Paediatrics and Child Health*, 56(5), 818–820. <https://doi.org/10.1111/jpc.14849>

Vaidyanathan, A. K. (2022). Controlling bias in research. *Journal of Indian Prosthodontic Society*, 22(4), 311–313. https://doi.org/10.4103/jips.jips_405_22

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425.

<https://doi.org/10.2307/30036540>

Venkatesh, V., Viswanath, & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, 39(2), 273–315.

<https://doi.org/10.1111/j.1540-5915.2008.00192.x>

Venkatesh, V., Viswanath, & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186–204. <https://doi.org/10.1287/mnsc.46.2.186.11926>


Venkatesh, Viswanath, Thong, J. Y., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, 17(5), 328–376. <https://doi.org/10.17705/1jais.00428>

- Vinnychuk, O., Vinnychuk, I., & Biloskursky, R. (2022). Conceptual fundamentals of practical application of Business Analysis. *Scientific Bulletin of Kherson State University. Series Economic Sciences*, (45), 69–75.
<https://doi.org/10.32999/ksu2307-8030/2022-45-9>
- Voruganti, K. K. (2024). Orchestrating Multi-Cloud Environments for Enhanced Flexibility and Resilience. *Journal of Technology and Systems*.
<https://doi.org/10.47941/jts.1810>
- Wang, J. (2021). A review of the development of the integration strategy of Information Technology and education in the four countries of the United States, Britain, China, and Singapore. *Science Insights Education Frontiers*, 9(2), 1283–1303.
<https://doi.org/10.15354/sief.21.re042>
- Wang, Q., & Xue, M. (2022). The implications of expectancy-value theory of motivation in language education. *Frontiers in Psychology*, 13.
<https://doi.org/10.3389/fpsyg.2022.992372>
- White, M. G. (2020). Why human subjects research protection is important. *Ochsner Journal*, 20(1), 16–33. <https://doi.org/10.31486/toj.20.5012>
- Xue, L., Rashid, A. M., & Ouyang, S. (2024). The unified theory of acceptance and use of technology (UTAUT) in higher education: A systematic review. *Sage Open*, 14(1). <https://doi.org/10.1177/21582440241229570>
- Yamcharoen, P., Bayewu, A., T.P., O., & Fatoye, O. E. (2022). Evaluating state cybersecurity laws and regulations in United States. *Advances in Multidisciplinary & Scientific Research Journal Publication*, 8(3), 47–56.

<https://doi.org/10.22624/aims/v8n3p4>

- Yoon, S. W., & Chae, C. (2022). Research topics and collaboration in human resource development review 2012–2021: A bibliometrics approach. *Human Resource Development Review*, 21(1), 24–47. <https://doi.org/10.1177/15344843211068807>
- Younas, A., Fàbregues, S., Durante, Á., Escalante, E., Inayat, S., & Ali, P. (2023). Proposing the “MIRACLE” narrative framework for providing thick description in qualitative research. *International Journal of Qualitative Methods*, 22. <https://doi.org/10.1177/16094069221147162>
- Zwitter, A. J., & Hazenberg, J. L. (2020). Decentralized network governance: Blockchain technology and the future of regulation. *Frontiers in Genetics*. DOI: <https://doi.org/10.3389/fbloc.2020.00012>

Appendix A: CITI Certifications



CITI PROGRAM

Completion Date 18-Sep-2022
Expiration Date N/A
Record ID 51577854

This is to certify that:

Allan Arroyo-Melendez

Has completed the following CITI Program course:

Not valid for renewal of certification through CME.

Student's
(Curriculum Group)
Doctoral Student Researchers
(Course Learner Group)
1 - Basic Course
(Stage)

Under requirements set by:

Walden University

CITI
Collaborative Institutional Training Initiative
101 NE 3rd Avenue, Suite 320
Fort Lauderdale, FL 33301 US
www.citiprogram.org

Generated on 09-Aug-2024. Verify at www.citiprogram.org/verify/?wc9a94053-4d4d-432c-bdd0-2dd46dc90b48-51577854

Appendix B: Interview Protocol

1. Thank you for your willingness to participate in the interview process for my doctoral research study. My name is Allan E. Arroyo-Melendez, and I am a doctoral student at Walden University. I am studying the Strategies IT Managers use to Implement a DRP and BCP after a cyberattack to improve the recovery time.
2. Participation in the interview is entirely voluntary.
3. I will ask for permission from the participants to switch on the audio recording, noting the interview's time, date, and location.
4. I will maintain each participant's confidentiality and privacy by omitting the participants' names and the organization from the transcript and any published data findings from the study.
5. The interview will last about 30 to 40 minutes, and the interviewee will be asked to respond to 9 questions.
6. Some follow-up questions may surge from the initial questions for more precise details.
7. Once the interview is over, the participants will be thanked for cooperating in the research with the interview.

All participants will be informed that I will contact them in about one or two weeks for a follow-up member-checking meeting with the interview transcript to discuss their feedback and comments, which will last around 15 to 30 minutes.

10. What cybersecurity strategies would you use to implement DRP and BCP after a cyberattack?

11. Have you ever participated in any DRP and BCP implementation after a cyber-attack? #Please describe the experience that would be a follow-up.
12. What are the key barriers to implementing DRP and BCP after a cyber-attack on an organization?
13. What steps do you take to ensure DRP and BCP policies will not interfere with job performance?
14. What steps do you take to simplify the execution of DRP and BCP?
15. How would you mitigate potential outside attitudes toward a particular DRP or BCP policy?
16. How would you improve the attitude toward DRP and BCP so staff may adopt these policies?
17. What importance do external factors such as laws, regulations, and privacy play in implementing a DRP and BCP after a cyberattack?
18. What additional strategies would you use for implementing DRP and BCP after a cyberattack?