2020

Strategies for the Development of IT Disaster Recovery Plans in the Manufacturing Industry

Michael Landry Sartwell
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Michael L. Sartwell

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. Betsy Macht, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Alexandre Lazo, Committee Member, Doctor of Business Administration Faculty

Dr. Mary Dereshiwsky, University Reviewer, Doctor of Business Administration Faculty

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

Walden University
2020

Abstract

Strategies for the Development of IT Disaster Recovery Plans in the Manufacturing Industry

by

Michael L. Sartwell

MBA, Columbia Southern University, 2014

BS, Columbia Southern University, 2010

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration - Homeland Security

Walden University

February 2020

Abstract

Information technology (IT) leaders have reported technology disruptions because of natural disasters, terror attacks, or adversarial threats. Information technology leaders are concerned with technology disruptions, as these disruptions are costing organizations as much as $22,000 per minute. Grounded in Zachman's framework, the purpose of this qualitative multiple case study was to explore strategies IT managers in the manufacturing industry use to develop IT disaster recovery (DR) plans to support business operations. The participants included 3 manufacturing IT professionals, 2 Department of Defense manufacturing infrastructure specialists, and 1outsourcing contractor, each from firms located in the central United States who successfully developed IT DR plans to support business operations. Data collection comprised of interviews and documentation. I used Braun and Clarke's (2006) six-step process for thematic analysis to identify 5 themes: contingency planning by priority, testing plans, levels of recovery, time requirements for recovery, and costs associations. The implications for positive social change include the potential for IT managers and leaders to contribute to strategic development of IT DR plans and prevent economic disruption for consumers, communities, and society during disaster events.

Strategies for the Development of IT Disaster Recovery Plans in the Manufacturing Industry

by

Michael L. Sartwell

MBA, Columbia Southern University, 2014

BS, Columbia Southern University, 2010

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration – Homeland Security

Walden University

February 2020

Dedication

The doctoral experience has been one of the most daunting tasks of my life next to combat and fatherhood. That said, I dedicate this study to my beautiful wife Cristy J. Sartwell and my children Kennedy, Landry, Jake, and Mikenzzie Sartwell. The support from my wife and children has been nothing short of admirable. My wife, an expert in time management, ensured I had scheduled space to focus on my studies, as she multitasked operations of her own business, daily home management activities, and family events. At the end of the day, my family made this dream come true for me and I am extremely proud of them for their sacrifice in order to allow me to complete my life goals. I love you all very much.

Acknowledgments

Completing the DBA program has been a goal of mine for the last several years. This would not have been possible without the mentorship and guidance of my advisor and chair Dr. Macht, and Dr. Krista, my former chair. It is because of their patience, experience, and support that I was able to push through the most challenging of times. There are no words that express my gratitude for your valuable time during this process. Thank you!

I would also like acknowledge the following network of advisors, friends, and mentors that kept me motivated during this process: Charlie Hausman, Kevin Fujimoto, Jeffrey Crane, George Acree, Ryan Jennings, Marie Watkins, Kent Martin, Samantha Clapper, Brian Graves, Don Lilleman, Robert McCormack, and Andrew Schueller. Thank you for your professionalism, patience, and understanding with words of encouragement through my life and career and in some cases a swift kick in the right direction.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

According to Cook (2015), if one does not prepare, then one fails to manage. Business continuity planning (BCP) is a critical process that organizational leaders use to engage in the strategic development of information technology (IT) disruption recovery planning in the event of a terror attack or natural disaster. Seventy-five percent of businesses without a BCP plan will fail three years after a disaster event occurs (Cook, 2015). Areas of strategic concern, typically included in BCP development, entail business plans, personnel plans, processes, policies, procedures, projects, and support systems (Cook, 2015). Organizational leaders use IT as the platform to support the supply, tracking, defense, analysis, and security of organizational networks and internal communications. Managers can review IT networks and support platforms to develop counter mitigations to risks and vulnerabilities found in the organization, which will support the resiliency of the BCP and the IT disaster recovery plan.

Background of the Problem

When developing strategic IT recovery plans, managers consider areas that include related policies and procedures, technology use, risk mitigation, employee negligence, technical safeguards, and budget management (Strauss, 2015). Additionally, managers must consider priority issues, such as criminal attacks, computer loss, and employee negligence, during development of response and recovery planning (Strauss, 2015). Leaders find vulnerabilities at every level of the organization that occur in areas of prevention, response, and recovery of IT.

Organizational leaders base strategic IT recovery plan elements on the type of organization (e.g., manufacturing, e-commerce, services, and retail) and the internal and external incident vulnerabilities specific to the business enterprise (Brown, 2016). Additionally, managers must identify specific responses for a given type of organization (e.g., manufacturing) to identify the needed response and associated costs (Brown, 2016). According to Brown (2016), costs for strategic IT recovery planning in areas of IT security, prevention, response, and recovery far outweigh the costs to organizations without an IT recovery plan. However, some managers place a lower priority on development of IT recovery plans because of expense (Brown, 2016).

Problem Statement

Firms that do not have an IT disaster recovery (DR) plan can incur a considerable loss when leaders face a crisis, thereby causing significant harm to a business organization during a fabricated or natural disaster (Mathaisel, 2017). On average, technology-related downtime in production can cost firms as much as $22,000 per minute (Stich et al., 2015). The general business problem is that some managers do not prioritize the development of IT disruption recovery strategies, potentially leading to the loss of millions of dollars. The specific business problem is that some IT managers in the manufacturing industry lack effective strategies to develop IT disaster recovery plans to support business operations.

Purpose Statement

The purpose of this qualitative multiple case study was to explore effective strategies that some IT managers in the manufacturing industry use to develop IT disaster recovery plans to support business operations. The population consisted of six IT professionals in manufacturing located in the central region of the United States who have knowledge of IT disaster recovery plans. The implications for social change include the potential for manufacturing leaders to gain knowledge of ways in which to develop IT disaster recovery plans that one may use to minimize disruption in the daily lives of consumers and communities during fabricated, terrorist, and natural disasters.

Nature of the Study

I selected a qualitative research method for this study. Researchers use a qualitative method to concentrate on functional and theoretical results or discoveries, based on research questions that they have developed through field study in normal environments (Park & Park, 2016). A qualitative method is suitable for this study because I utilized a multiple case study design and interview participants in order fully explore effective strategies used by IT managers in the manufacturing industry to develop IT disaster recovery plans. Additionally, according to Franco (2016), a qualitative method is appropriate for case study research as viewed through an assigned conceptual framework in order for the researcher to expand and reflect changes from a pragmatist perspective; that is, one who is mindful of abundant research practices with reverence to their worth of a research subject. Furthermore, qualitative methodology is in its purist form a catalyst for the researcher to collect descriptive data from participants in their own words and records behaviors tied to a research subject. In this case, as the researcher using qualitative methods, I collected descriptive data from participants to reflect effective strategic outcomes related to IT disaster recovery plans (Tyalor, Bogdan, & DeVault, 2016). Researchers use quantitative methods to collect data through surveys, and then translate the data numerically to examine differences in variables to test a hypothesis (Patten & Newhart, 2017). A quantitative method was not suitable for this study because I did not examine relationships between variables or testing hypotheses. Researchers use a mixed method approach to combine qualitative and quantitative methods in a study, and then triangulate among the associated variables (Turner, Cardinal, & Burton, 2015). A mixed method approach was not suitable for this multiple case study because I did not use a quantitative method to explore IT disaster recovery strategies.

Researchers use several types of qualitative study designs. These include the use of a case study design to develop an in-depth description and analysis of a case research subject to explore *what, how,* or *why* research questions (Yin, 2017). A case study design was suitable for this study because I explored ways in which IT managers develop and implement disaster recovery plans. Researchers use an ethnographic design to describe cultural themes in a group of people through long-term observation (Eisner, 2017). An ethnographic design was not suitable for this study because it did not involve the study of a culture or cultural needs. Researchers use a phenomenological design to research the essence of experiences and to examine a lived experience using descriptive, interpretive, and narrative applications (Levitt, Motulsky, Wertz, Morrow, & Ponterotto, 2017). A phenomenological design was not appropriate for this study because I did not examine a lived experience or the essence of experiences (Giorgi, 2017). Narrative design, in which the researcher focuses on individual stories arranged in sequential order and related over time (Walliman, 2017), was also not suitable for this study because I did not examine individual stories.

Research Question

What effective strategies do some IT managers in the manufacturing industry use to develop IT disaster recovery plans to support business operations?

Interview Questions

1. How did you identify effective strategies for developing IT disaster recovery plans?
2. How did you assess the effectiveness of these strategies for developing IT disaster recovery plans?
3. What key obstacles did you encounter to the implementation of strategies to develop IT disaster recovery plans?
4. How did you overcome these obstacles to the implementation of strategies to develop IT disaster recovery plans?
5. How have your organization's IT disaster recovery plans impacted business operations?
6. What additional comments or information regarding effective strategies to develop IT disaster recovery plans would you like to provide that you have not already shared?

Conceptual Framework

The conceptual framework for this study is Zachman's (1987) model concerning enterprise information systems (EIS) design, implementation, and operation. Zachman created this model as a mechanism for understanding the complexity of relationships between information technology, people, and data systems (Lapalme et al., 2016). The ontology of the Zachman (1987) model includes the *what, how, where, who, when,* and *why* dimensions of EIS operations. The *what* dimension refers to data stored in the EIS. The *how* dimension applies to the software applications in the EIS. The *where* dimension relates to the computer network hardware infrastructure. The *who* dimension aligns the EIS with managers responsible for IT disaster recovery plans. The *when* dimension denotes event lists, models, and diagrams that specify timelines and reactions to EIS failure. The *why* element relates to the requirements and goals needed to produce disaster recovery within IT systems. I use the Zachman model as a lens for describing ways in which IT managers identify and implement strategies for the development of IT disaster recovery plans.

Operational Definitions

Business continuity plan (BCP): A crucial risk management-planning tool that organizational leaders use to recover from a natural or fabricated crisis (Hatton, Grimshaw, Vargo, & Seville, 2016). Leaders use the BCP as a strategic benchmark for overall business competitiveness and longevity to ensure organizational resiliency, while experiencing a significant disaster event (Hatton et al., 2016).

Disaster recovery (DR): The preparation process for continuation of organizational systems essential for enterprise survival (Banerjee & Biswas, 2017). DR includes a focus on IT systems and specific control measures in three critical areas: preventive, detective, and corrective (Banerjee & Biswas, 2017).

Disaster recovery plan (DRP): Organizational leaders use this term to outline strategies to reconstitute raw technical data from secondary systems and react quickly to replicate IT sources using stand-by applications dedicated before a disruption (Cervone, 2017; Ferrari, 2016).

Enterprise architecture (EA): Applications that organizational leaders use to streamline and improve management and complex functions specific to organizational needs and information system requirements (Lapalme et al., 2016).

Enterprise information system (EIS): All information systems, including human resources, information technology, and design applications (Lapalme et al., 2016).

IT Governance: Managers use this term as a system to direct and control usage within an organization governed by the International Standard for Corporate Governance of Information Technology (i.e., ISO/IEC 38500, 2008) in areas of IT business strategy, IT capability, and IT operations within the business platform (Juiz & Toomey, 2015).

Supply chain integration: A set of activities that managers use with the coordination of product flows between supply chain partners, transactions, material movements, procedures, and optimization processes, considering the underlying information flows (Vanpoucke, Vereecke, & Muylle, 2017).

Supply chain management (SCM): Leaders use this application term as a supply network to coordinate relationships with suppliers and customers that add overall value to the enterprise and lower costs for the procurement of upstream and downstream distribution of materials that they manufacture into products for customers (Agus, Hassan, & Ahmad, 2017).

Assumptions, Limitations, and Delimitations

Assumptions

Marshall and Rossman (2016) described an assumption as an element of research one assumed true and not proven. I have four assumptions in my study. First, I assumed that participants interviewed answered the research questions truthfully and provided the best answer possible based on their expertise. Second, I assumed that leaders within the manufacturing industry lack strategies for developing IT disaster recovery plans. Third, I assumed participants interviewed were IT technical experts within the manufacturing industry. Finally, I assumed my findings would give a positive contribution to the manufacturing industry through exploring my research question.

Limitations

Research limitations are weaknesses within a study that may constrain the output of the project findings (Madsen, 2013). While there may be standard processes one uses to develop strategic IT response, manufacturing leaders may have different needs depending on types of products, size, sample diversity, and technical requirements needed. A second limitation is that I used only one central framework as a lens for exploring my study topic. Using the Zachman (1987) framework as the only conceptual model may conflict with other related frameworks that will present different outcomes. I openly define the basis of my research and compare other conceptual frameworks that researchers have used to develop IT recovery strategies.

Delimitations

Delimitations are research boundaries used by researchers to define the scope of a project (Becker, 2013). The first delimitation is that I focused on a multiple case study approach concerning participants who had knowledge of manufacturing located in the central United States. Secondly, I included only subject matter experts in the field of IT to expand strategic development of IT recovery in a crisis.

Significance of the Study

Contribution to Business Practice

DR planning is the foundation of organizations in any capacity to maintain seamless function in a crisis. Managers use IT disaster recovery plans as standard operating procedures to incorporate risk mitigation processes, align public and private partnerships, and articulate business goals associated with cultural environments (Carden, Boyd, & Valenti, 2015). Snell (2015) stated that a key to IT disruption prevention includes one encouraging behavior that sets high expectations for employees, business partners, and contractors to follow technology disruption prevention and response protocols.

While the consumer lives in a world of extreme technological dependence, business organization leaders rely on IT operations and technical managers for day-to-day services and deliverables. The identification of strategies for the development of IT disaster recovery plans may enable IT managers and organizational leaders to maintain business operations, deflect brand degradation, and ensure supply chain relationships. Additionally, information regarding strategies for the development of IT disaster recovery plans may enable businesses to become more resilient during a natural or fabricated catastrophic event.

Implications for Social Change

The implications for social change include the potential for IT managers in the manufacturing industry to learn of IT disaster recovery plans that may help them prevent economic disruption for consumers, communities, and society during crisis events (Cook, 2015). For example, successful IT disaster plans may positively influence customers who rely on an enterprise to have continued access to products and services (Cook, 2015). Additionally, manufacturing business leaders with successful IT disaster recovery plans may contribute to the economic stability of communities by enabling the continued production and distribution of goods during crises. Furthermore, members of society may gain a sense of security knowing that firms, supplying critical products, have IT disaster recovery plans in place.

A Review of the Professional and Academic Literature

This section includes a review of the professional and academic literature related to the problem statement and purpose of this study. A reader can use the literature review to understand a comprehensive and current analytical examination of the theme, while the researcher succinctly provides an in-depth knowledge base regarding a given subject of study (Galvan & Galvan, 2017). Using Google Scholar, ACM, EBSCOhost, and ProQuest, I conducted an exhaustive literature review concerning strategies to recover IT applications within the manufacturing industry during a fabricated or natural disaster. I used the following keywords to conduct this review of the literature: *supply chain* *network, manufacturing software, IT network infrastructure and communication, IT governance, IT contingency planning, IT strategy requirements,* and *Zachman's (1987) framework for enterprise architecture (ZFEA)* concerning *enterprise information systems (EIS)*. I retrieved information on the subject areas from 65 sources comprised of 65 (100%) peer-reviewed articles, with 60 (92%) of the total references published between 2014 and 2018. I used the ZFEA as a lens to support my requirement to establish a conceptual platform for strategic IT recovery planning. Additionally, I used ZFEA to help me expand on the *what, how, where, who, when*, and *why* used to develop IT disaster recovery plans.

The *what* aspect of ZFEA model assisted me in exploring data used to manage supply chain operations related to IT in manufacturing. I used the how portion of Zachman's (1987) model to describe manufacturing software applications within enterprise. I used the *where* characteristic of ZFEA to assist me in presenting locations of IT network infrastructures and communications within IT recovery plans. I used the *who* component of ZFEA to support my illustration of the existence of IT governance through managerial responsibilities. Additionally, I used contingency planning research to aid me in portraying the inputs, reactions, and timelines for describing the *when* portion of the ZFEA model. Finally, I used the *why* of the Zachman model to explore strategies for IT disaster recovery in the manufacturing industry.

Supply Chain Networks (ZFEA *What*)

One critical area important to manufacturing business is supply chain operations. Leaders use different IT applications to manage the supply chain (SC) process essential for organizational production. In March of 2011, an earthquake known as *The Great East Japan Earthquake* (GEJE) struck Japan's Pacific coast, thereby causing a devastating tsunami that researchers have identified as the most significant natural disaster to ever influence SC operations (Hendricks, Jacobs, & Singhal, 2017). Hendricks et al. (2017) found that not only did the hurricane harm 6,000 factories, but the overall share value also decreased by 3.73% on average because of performance issues experienced by firm leaders. This documented reaction—termed the contagion effect among suppliers or a response to the SC networks associated with the affected companies—is the main reason for the adverse returns for over 95% of businesses at ground zero (Hendricks et al., 2017). Associated SC providers must have alternate suppliers during a disaster event. Software engineers create IT applications that supply-manufacturing networkers use to buy, sell, deliver, track, and manage workflow systems and provide organization resiliency through IT recovery platforms. Additionally, managers use these recovery plans to gain a competitive advantage against other company leaders who may otherwise close during a crisis (Vanpoucke et al., 2017). This research illustrates the importance of supply chain operations to the manufacturing business.

Researchers have examined the essential components of SC systems. Azadegan and Jayaram (2017) separated SC systems into three organizational characteristics related to resiliency: (a) inherent resilience (system strengths), (b) anticipative resilience (preparatory capabilities), and (c) adaptive resilience (coping). Company personnel incorporate these three resiliency traits into IT response and recovery efforts during a disaster event. When looking at recovery strategies, one must understand the system managers have used. SC technology systems are a vital platform for organizational survival. Depending on the needs of the organization, business leaders must develop continuity plans to outline strengths, preparatory capabilities, and coping mechanisms for strategies of IT disaster response efforts (Azadegan & Jayaram, 2017). Business leaders use SC technology systems as a catalyst for systems theory and employ the family resilience model to enhance resiliency aspects within supply networks (Azadegan & Jayaram, 2017; Lapalme et al., 2016). Supply chain operations are a vital component of a manufacturing firm's survival during a disaster event. Additionally, managers require IT recovery plans that they can use to decrease supply disruption. Therefore, leaders use IT recovery plans to reduce consumer dissatisfaction and lessen the associated financial costs.

As research has progressed on this topic, scholars have explored theoretical implementations of disasters and their effects on supply chains. For example, Balza-Franco, Paternina-Arboleda, Cantillo, Macea, and Ramírez-Ríos (2017) applied the game theory approach to assessing cost strategies used during natural and fabricated disasters. Balza-Franco et al. found that teams using the game theory method could lower costs associated with supply chain networks, which could optimize supply resources pre and post disaster. According to Balza-Franco et al., managers and leaders reorganize supply chain networks and associated costs during a disaster using one of the three following planning strategies: (a) no-cooperation (NC), (b) decentralized cooperation (DC), and (c) centralized cooperation (CC). Business leaders prefer the centralized planning strategy to provide supplies and raw materials to the manufacturer more quickly, thereby supporting product demand (Balza-Franco et al., 2017; Benner & Pastor, 2015). Balza-Franco et al. (2017) found that organizational leaders developed tactical continuity models to establish pre-allocated warehousing supported by assigned allocation centers (e.g., airports, terminals, and stations). Managers use allocation centers to serve as general support and nodes for distribution (NFD) of supplies to predetermined areas linked to production requirements (Balza-Franco et al., 2017; Tian, Zhao, Xu, Zhong, & Sun, 2015). For these processes to work efficiently, logistic suppliers and related business stakeholders should maintain common interests. Similarly, these authors identified a critical predisaster strategy as the need to collaborate among manufacturing supply chain networks in areas of production, transportation, acquisition, warehousing, and transportation requirements. Managers use this collaboration to lower organizational costs associated through deploying an IT recovery plan. Leaders use collaboration concepts to refine expenses, lower risks related to disaster events, and create strategies to enhance organizational resiliency.

Leaders use a technical application, known as supply chain management (SCM), to track supply and demand, production, transportation, facility, and distribution. Additionally, managers use SCM to develop IT disruption and recovery strategies for organizational networks during a fabricated or natural disaster (Khalili, Jolai, & Torabi, 2017; Tabaklar, Halldorsson, Kovacs, & Spens, 2015). According to Khalili et al. (2017), a two-stage concept, tied to IT management tools, incorporates simultaneous handling of operational vulnerabilities from a logistic perspective in areas of risk mitigation and recovery planning. In the first stage, managers and leaders decide the structure of the supply chain and review associated risk mitigations, while the second phase requires them to specify the recovery plan of lost capability to production and distribution networks (Khalili et al., 2017). Managers use the two-stage concept during related fabricated and natural disasters to develop specific strategies for a particular type of manufacturer and their specific location, thereby intuitively helping leaders of that organization establish IT recovery plans dealing with specific supply chain networks (Khalili et al., 2017). These findings reflect the increasing use of technology to monitor supply chain management.

Researchers have also begun to apply technological developments to planning and anticipating change in regard to supply chain management. Developers have combined technology within SCM and enterprise resource planning (ERP) to support successful supply chain operations (SCO) and logistic network activities (Acer, Zaim, Isik, & Calisir, 2017). Because of this combination, managers of firms should ensure they hire the best IT experts possible to operate information systems; failure to do so can cause a loss of utilization in ERP and SCM functions, thereby creating disadvantages to organizations (Acer et al., 2017). When creating IT disaster response plans, leaders should incorporate the top IT professionals as a strategy to manage upstream and downstream supply partners adequately during a crisis. Underutilization of IT systems can cause a lag in operational performance, risk to recovery of lost capabilities, and a loss of overall resiliency to workflow systems amid a disaster event (Vanpoucke et al., 2017). These findings reflect the evolving role of technology in supply chain management.

Supply chain Integration (SCI) includes operational performance, information exchange (i.e., transfer of communication), and supplier selection (i.e., collaboration, decision-making, and developments) about IT use in manufacturing organizations. Leaders can use SCI to affect upstream and downstream supply networks positively, thereby resulting in lower costs, maximum distribution applications, and process elasticity (Vanpoucke et al., 2017). IT managers use different enterprise networks to strengthen the exchange of information between the buyer and supplier, therefore causing a reduction in lead times related to more efficient processes for ordering and selecting suppliers among firms (Vanpoucke et al., 2017). One can use supply management IT solutions to bolster sales in the manufacturing industry as another fundamental concept to rapid recovery during a fabricated or natural disaster (Argus et al., 2017). These findings show that IT is increasingly important in promoting efficiency in the manufacturing industry.

Researchers have also begun to explore ways in which to measure supply chain management more effectively. One can measure supply chain and management sales as having significant relationships between SCM, customer relations practice (CRP), technology, and information sharing (IS) with suppliers in manufacturing companies (Argus et al., 2017; Tatoglu et al., 2016). Supply management has a significant influence on sales in manufacturing firms through customer relations, technology and innovation, and strategic sharing of supply chain partners (Argus et al., 2017; Tatoglu et al., 2016). A strategic balance between sales, customers, and manufacturing exists within the supply chain practice (Argus et al., 2017). Therefore, incorporating alternate IT solutions to ensure stability among these factors is a priority during a crisis event.

Leaders use the *what* dimension of the ZFEA framework to develop strategic IT recovery plans. Managers use the strategic plans to create subordinate categories within the supply chain network that must remain resilient during a crisis (Ivanov, Pavlov, Dolgui, Pavlov, & Sokolov, 2016; Lapalme et al., 2016). Specific areas of priority for IT recovery strategies include (a) SC risks, (b) SC vulnerabilities, (c) production, (d) distribution operations, (e) required costs transactions associated with SC network, and (f) information systems maintenance. Managers and leaders who use these areas as a basis to develop recovery strategies for EIS supply chain related networks can construct IT recovery plans to add resiliency to manufacturing firms during a crisis. At every level, leaders and managers must know and understand how the different software applications work in a manufacturing organization to develop strategic recovery planning within EIS.

Manufacturing Software (ZFEA *How*)

Managers use software to create processes under the how aspect of the ZFEA model related to the manufacturing business procedures. To a manufacturing company, software is the epicenter of the operational process. Leaders use many applications to facilitate enterprise processes. Managers have developed some of these technical illustrations from cloud orchestration, cloud-based infrastructure, security applications for Internet of things (IoT), and engineering software (Banerjee & Biswas, 2017; Dunne & Malone, 2016; Landwehr et al., 2017; Pan, 2017). Managers use a new technical software product, called cloud orchestration software (COS), to apply multiple electronic backup sites that they have linked to a central supporting server (Banerjee & Biswas, 2017). Managers use COS software to prioritize network areas that require server backup during a crisis in IT disaster recovery (DR). Managers use COS to find the correct recovery capability needed by reviewing DR workload, characteristic, tenant requirements, and skill needs to network multiple secondary sites (Banerjee & Biswas, 2017). Managers use the newly patented application to issue efficient workloads required for failed sites during a DR event. Additionally, leaders use COS to find multiple site requirements for each type of workload needed to recreate the application from the best site available from previously designated sites that support the manufacturing process (Banerjee & Biswas, 2017). These findings show the increasing role software plays in the manufacturing industry.

Managers in the manufacturing industry have also begun to take advance of the cloud for various purposes. Managers use cloud-based infrastructure to enhance recovery capability for small and medium enterprise to maintain a high level of resiliency during an outage, while remaining cost effective (Dunne & Malone, 2016; Garrison, Wakefield, & Kim, 2015). Leaders use this type of application to focus on time needed to restore system operational resources within the cloud for an on-demand service obligation (Dunne & Malone, 2016; Garrison et al., 2015). Additionally, managers also need strategic applications, such as COS, to secure electronics, software, and sensors people have used to keep upstream and downstream supply operations resilient against DR.

As manufacturing businesses have taken advance of the cloud, security has also become a concern. Pan (2017) explored the need for security strategies for IoT networks (i.e., electronics, software, and sensors) that allow managers to develop IT recovery plans derived from analyzing design to production aspects in manufacturing that reveal processes vulnerable to cyberattack. According to Pan, the more common problems resulting from cyberattack in a manufacturing organization include tampered digital filings, changes to mechanical properties resulting in part failure, increased manufacturing costs due to defects, and possible loss of life depending on where the manufactured part exists on the line. Pan expanded on vulnerabilities within IoT applications that managers could mitigate. Managers can use risk information to create inspection criteria to defend better against an attack to a network related to manufacturing workflows (e.g., product design, raw materials, assembly, inspection, and distribution) (Zou, Kiviniemi, & Jones, 2017). Managers use the logical flow process in manufacturing to detect security vulnerabilities in IoT (see Figure 1).

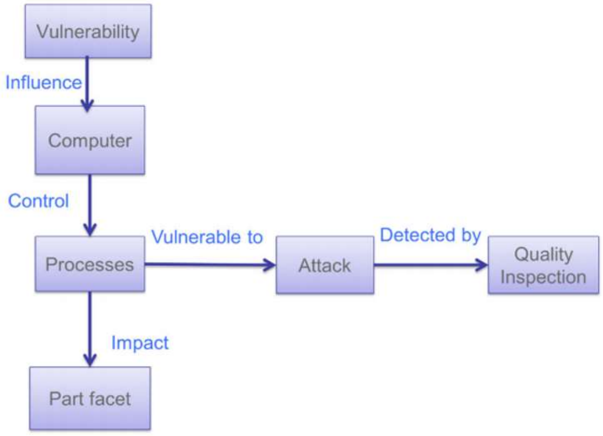


Figure 1. Logic flow in manufacturing processes. Adapted from “Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems,” by Y. Pan, 2017, *International Journal of Interactive Multimedia and Artificial Intelligence, 4*, pp. 45-54. Copyright 2017 by Universidad Internacional de La Rioja (UNIR).

Managers and leaders use the ZEFA model to secure vulnerabilities strategically within IoT based manufacturing organizations and create the required IT response to weaknesses, such as a compromised worker, operating system (OS) software, and weak authentication processes (Chang, Kuo, & Ramachandran, 2016; Pan, 2017). In manufacturing organizations, managers analyze and mitigate other areas of attack, such as attack vectors, attack targets, attack impacts, confidentially attacks, availability attacks, and integrity attacks (such as material and structural attacks; Chang et al., 2016; Pan, 2017). Technology researchers, such as Pan (2017), provide manufacturing leaders with updated information on strategic recovery planning. Additionally, technology researchers can help organizational staff have more capabilities of planning DR to create better prevention measures for an attack on IoT systems and technical infrastructures.

IT Network Infrastructure and Communication (ZEFA, *Where*)

Another important topic influencing the manufacturing industry is the development of efficiency infrastructures and communication networks. Lapalme et al. (2016) expanded the ZEFA method regarding the EIS for designing and operating IT systems within an organizational infrastructure. Managers and engineers conduct and construct network infrastructure within the manufacturing business operation to enable communication between standard business processes and supply chain systems. Under the Zachman (1987) model, managers use the EIS platform to review strategic technology systems to manage inputs and outputs of the manufacturing organization. Leaders control some of the following data and outputs: RiskRoute framework, IS, LIS, ERP for networks, technology sustainment, and opportunities of information systems or the lack thereof.

RiskRoute Framework. The physical routed infrastructure of network wire location, length, and capability is an aspect of strategic IT response development. The RiskRoute framework is an optimization framework that one can use to permit backup bit-mile (i.e., air mile) network routes to react to both past and instantly forecasted connectivity disruptions along a single air mile (Eriksson, Durairajan, & Barford, 2013; Sun, Karwan, & Kwon, 2015). Following Hurricane Katrina, no backup system was in place for many miles of underground RiskRoute cabling within the affected geographical area. Because of the lack of RiskRoute frameworks plans, New Orleans populace had no Internet conductivity for months, leaving local organization leaders without the ability to communicate digitally and disrupting the enterprise Internet connectivity. Leaders and managers use RiskRoute infrastructure to plan for backup paths, route variations, delivery recommendations, and new paring connections, which diminish risk of disruption to IT networks (Erikson et al., 2013). This framework is one example of how a natural disaster has led to enhanced IT responses in the manufacturing industry.

Information systems (IS). Managers use IS to control technical outputs in all areas of business or, in this case, the manufacturing industry. Leaders can use IS technology to plan the development of professional concepts and techniques. Managers use this method as the catalyst to plan and organize data, communicate between the client and IS, and implement IS strategies (Cassidy, 2016; Wolf & Floyd, 2017). Managers use IS strategic planning to establish support techniques and bring together the entire organization under one succinct direction (Cassidy, 2016; Wolf & Floyd, 2017). Leaders use strategic IS architecture to secure enterprise, protect company investments, and deliver multi-level managers together to enhance business operations (Cassidy, 2016; Wolf & Floyd, 2017). Managers must understand the workings of IS strategy, regarding leader collaboration in all parts of the organizational environments, to set the stage for IS recovery and response during a crisis event. Leaders must strategically create IS to react well to different disaster events for organization survival during a fabricated or natural disaster.

Logistic information systems (LIS). The LIS is used as a priority technology for supply applications needed in the manufacturing industry. Managers use LIS as a process to network differences between logistic applications for outbound/inbound products and materials to the manufacturer, the warehouse, and then to the consumer (Bookbinder & Dilts, 2016; Lauras, Truptil, Charles, Ouzrout, & Lamothe, 2017). Managers use this type of system to rely on the needs of the customer in all respects (i.e., consumers and manufacturing customers), termed the just-in-time (JIT) requirement for coordination and supply (Bookbinder & Dilts, 2016; Lauras et al., 2017). Managers develop recovery strategies for LIS/JIT systems to accomplish inbound/outbound material movements to keep the organization resilient against technology disruption. Leaders use additional strategies that support LIS/JIT in the areas of administration, production management, and marketing requirements.

Enterprise resource planning (ERP). Under the ERP structure, researchers have considered multiple areas, such as human resources, production, and marketing.

Managers use ERP to address strategic information planning (ISP) applications with lean organizational practices (Hong, Siau, & Kim, 2016). Managers use ERP due to benefits that include financial, lean inventory practice, and integration of different data systems to reduce overall costs and improve supply chain management systems. DeLone and Mclean (1992) created the IS success model to use in conjunction with ERP. Managers use the IS success model and ERP together to measure overall performance. Managers use the ERP aligned with business strategies to influence organizational input and output. Managers use ISP methodology to link the enterprise strategies in a phase-by-phase approach to enable IT systems to support business operations in two main areas. First, managers use ISP methodology to combine company and information strategies to create plans for IS implementation. Secondly, managers use ISP methodology to shape IS sharing to generate grander plans through application collaboration. Managers use ISP to protect ERP systems; if disrupted, managers must restore these systems to maintain big picture enterprise production in manufacturing. Managers use a strategic recovery requirement for ERP to answer the ever-changing complexities of system management and sustainment technology requirements.

Technology sustainment (TS). TS refers to the technical process of changing raw materials into a product of value via manufacturing. According to Black and Kohser (2017), manufacturing technology is the foundation of American industry. Managers use technical manufacturing systems to set physical placement of machines to operate under measured inputs and create an output. Additionally, all leaders who use TS operations, associated with the manufacturing process, have strategic IT recovery planned before a fabricated or natural disaster can occur (Paul, Sarker, & Essam, 2015). These findings reflect the importance of TS to modern manufacturing practice.

Opportunities for Technology. When leaders manage information systems with a worst-case strategic approach to IT recovery during a disaster event, they will strengthen the overall resolution of an organization. Managers need to know and understand ways in which information systems can help, hinder, or create opportunities (Dwivedi et al., 2015; Pearlson, Saunders, & Galletta, 2016). Additionally, managers who understand necessary technology concepts can develop strategic recovery plans to support decision-making; company staff can use these concepts to maintain continuity of organizations during a disruption (Dwivedi et al., 2015; Pearlson et al., 2016). Managers who understand information systems used in manufacturing will understand the need to develop strategic recovery plans to maintain continuity of their organizations during a disruption.

IT Governance (ZFEA, *Who*)

Technology subject matter experts in the manufacturing industry are vital to the success of operating systems. IT managers and leadership team members in every departmental field within an organization share responsibility for the development of IT recovery plans (i.e., IT governance). Managers and staff must develop IT disaster recovery plans as a team with different departments within the business to strengthen the resiliency of the organization during a disaster event. A diverse group and their subordinates must initiate this plan and adjust as needed to be successful. According to Lee, Swink, and Pandejpong (2017), manufacturing process innovation (MPI) refers to one linking diversity and technology maturity within teams to provide successful outcomes with information processing. Lee et al. (2017) discovered project teams faced positive and negative influences between process and product teams, which the researchers related to manufacturing. Managers can face issues with these combined teams when tasking a team to develop IT disaster recovery plans (Ozdamar & Ertem, 2015). Furthermore, Lee et al. (2017) stated group members require technology maturity and diversity of organizational knowledge. Therefore, managers must develop from all areas of an organization to create strategies for IT disaster recovery within the manufacturing industry.

Individual subject matter leaders in IT, organizational department managers, and related enterprise technology architecture experts blend the needed applications for positive business outcomes. IT governance (ITG) refers to a combination of process relationships, organizational behavior, strategy, and cultural norms ingrained into the enterprise IT network (Almeida, Linares, Pinto, Lourinho, & Silva, 2017). Managers have aligned specific areas of the ITG umbrella with resilient IT strategies as the development of best practice procedures, IOS standards, and intertwined IT frameworks (Almeida et al., 2017). ITG is a critical construct necessary for the success of an organization. According to Alreemy, Chang, Walters, and Wills (2016), managers use IT networks to reduce risk, create value, and expose critical success factors (CSF) related to the enterprise operation. The principle key is to know and understand the amount of CSF needed for an ITG network (Alreemy et al., 2016; Li, Chang, & Yen, 2017). To have resiliency, organization leaders must have ITG to manage goals and facilitate the competitive advantage. Managers use ITG to oversee processes, operations, associated plans, and tasks of the stakeholders to create initial source factors of ITG, known as SFITG (Alreemy et al., 2016; Li et al., 2017). Managers use SFITG to keep standards and frameworks relevant and implement ITG. ITG refers to a strategic platform that managers use in the successful development of IT disaster recovery plans (Alreemy et al., 2016). Specific factors that affect the IT recovery plan include standards implementation, extraction of CSF enablers, relevant sources, counter IT barriers, scope of the organization, and alignment of life cycle categories within an enterprise (Alreemy et al., 2016). ITG plays a key role in ensuring that IT is effective and efficient within the manufacturing industry.

Employee, boards, and performance relationships affect ITG and its construction as well. Turel, Lie, and Bart (2017) amplified the need for strategic factors to turn ITG into a conglomerate of organizational performance and board level alignments based on required IT architecture within an enterprise. The ITG structure contains four related strategic elements: employee responsibility, business opportunity, IT relationships that influence business goals and enterprise IT capability (Mijumbi et al., 2016; Turel et al., 2017). Managers have used successful IT networks are in the context and structure of an ITG format, along with a contingency theory approach to define strategic, operational, domain, and social alignment (Turel et al., 2017). Each of these factors are important in designing a general ITG model or framework.

IT Contingency Planning (ZFEA, *When*)

Contingencies are backup plans (e.g., key systems of an organization that leaders ensure are operational, therefore allowing managers to keep the business operational). Managers must implement organizational survival during a disaster that requires four principals: impact analysis, business continuity (BC), incident response (IR), and disaster recovery (Clark, 2010; Sahebjamnia, Torabi, & Mansouri, 2015). The contingency planning management team (CPMT) is a strategic group whose job involves analyzing by priority the different business processes to build contingencies to keep priority functions influenced during a disaster; the strategic group creates a business impact analysis plan (Clark, 2010; Sahebjamnia et al., 2015). For this study, I discuss all areas of contingency planning with a focus on the IT disaster response (DR) plan and strategies that managers and leaders use in manufacturing organizations to develop specific policies and critical concepts for backup systems.

Managers react to IT securing concerns in various ways. According to Clark (2010), managers react frequently to IT security related incidents of the fabricated type (e.g., viruses, denial of service, trojans, and worms). Using the disaster recovery plan, managers and teams protect data from all threats and vulnerabilities to personnel and equipment (Clark, 2010). Leaders use the Business Continuity Plan (BCP) to relate the previous planning in BC, IR, and DR concerning IT, to the extent the team can relocate an entire organization if needed (Torabi, Giahi, & Sahebjamnia, 2016). The way in which managers react can also influence team members' responses.

Teams use IT contingency planning to develop critical concepts for backup systems, reaction times, and responsibilities by leaders and managers in a disaster. Organizational teams build IT contingency plans based on resiliency methods that managers require when a disaster event occurs, thereby allowing leaders to provide fail-safe IT recovery plans for organizational resiliency. Researchers have linked all contingency planning to leadership teams' communication efforts in an organization (Hosseini, Barker, & Ramirez-Maruez, 2016). Xu, Sugumaran, and Zhang (2015) expanded critical concepts in IT communication to improve the precision and competence of emergency management systems through data processing operations and using simulation to implement IT recovery plans. Simulation testing is a principal concept used by leaders and managers for the strategic development of IT recovery plans during non-catastrophic periods (Li, Tao, Cheng, & Zhao, 2015; Xu et al., 2015). Teams use new technologies to help them provide solutions to longstanding emergency management concerns, specifically in significant data processing in organizations. Leaders use these techniques to not only save lives during emergencies but to also create resilient business enterprises, specifically in areas of IT communication planning, preparedness, response, and recovery (Xu et al., 2015). Leaders use simulations (like table-top-testing) of IT recovery to reduce technical barriers that managers have found during a real-world disaster (Xu et al., 2015). The leader, manager, and organizational team must use results of simulations testing to prepare the IT disaster response plan fully.

Managers use testing of IT recovery plans with every possible fabricated or natural disaster event as a strategic task to allow response teams the ability to strengthen emergency response efforts within crucial enterprise networks. Leaders who introduce high-level architecture (HLA) within IT platforms for disaster event simulations will enhance response and recovery planning (Erdejl, Natalizio, Chowdhury, & Akyildiz, 2017; Hwang et al., 2016). IT teams make decisions based on the reusability and extensibility of a strategic application to reduce confusion during a crisis when applying HLA applications to simulation exercises (Hwang et al., 2016). Managers conduct testing of disaster response measures in every possible scenario to develop strategic IT recovery plans fully. At every level of business operations, leaders and managers use integrated outcomes to create the strategic response and recovery plans, thereby creating backup contingency plans for large data applications within the enterprise (Hwang et al., 2016). Real and simulated disasters have assisted in the understanding of IT recovery plans.

Most business managers require teams who plan for quick IT recovery during fabricated or natural disasters with the ability to react appropriately to disrupted technical applications and to maintain system performance succinctly as the catastrophe occurs. Managers use distributed backup high-speed mass-data applications for teams to create in-memory slave server systems with the availability to backup, retrieve, and recover memory in an instant during a crisis event (Min, Hwang, Jang, Cho, & Hong, 2015; Wang, Ouyang, Li, & Liu, 2017). According to Min et al. (2015), teams who use this distribution recovery method improve performance during a catastrophic event by 51.4%. Min et al. further discussed one required such an improvement due to the increase of data availability on trusted multiple internal servers that reduced data recovery time to uphold performance. These findings illustrate the importance of having a plan in place to promote a quick disaster response.

IT Strategy Requirements (ZFEA, *Why*)

Strategy requirements can impact It disaster responses. Researchers have termed Hurricane Katrina (HK) as one of the five most deadly hurricanes in U.S. history (Bala, Venkatesh, Venkatraman, & Bates, 2016; Landry & Koger, 2006). HK made its first landfall 23 August 2005 in the Gulf-Port, Mississippi area, later making its second landfall in Southeast Louisiana on 29 August 2005 as a Category 3 hurricane. Labeled one of the worst disasters in U.S. history, HK devastated everything in its path and caused loss of life, property, and long-term economic damage for residents and business organizations alike (Bala et al., 2016; Landry & Koger, 2006). According to Landry and Kroger (2009), managers and leaders should consider all threats to an organization under a pessimistic lens to keep the firm more resilient by creating comprehensive strategies to assist in the development of IT disaster recovery plans within the industry. Researchers have used HK and many other disasters to develop lessons, learned risks, and vulnerabilities. Managers can use business continuity management (BCM) and IT disaster recovery planning as a strategy based on the strength, capability, and response requirement of an organization (Azadegan & Jayaram, 2017). This framework is a recent addition to the literature on IT disaster recovery and its impacts require further study.

While every geographical area is different, all people will suffer some type of disaster event. Therefore, business managers should have a strategic IT DR plan to aid in the following areas: organizational loss of power and hardware issues, set up of mock DR testing, security against attacks and hacks during a crisis, coordinated hot sites, adequate relocation resourcing, equipment availability, backup strategies across IT systems, and department involvement at all levels of internal and external leadership (Landry & Kroger, 2006; Yang, Yuan, & Huang, 2015). Leaders, managers, and teams apply this knowledge as the platform data needed to begin building strategic IT recovery plans.

Additionally, leaders who understand and use different theoretical approaches will let teams create diversity between elements of the project regarding various disaster scenarios. For example, some business leaders use game theory methods to plan for a crisis event to lower delays in performance when applied to cost and logistic resource requirements (Balza-Franco et al., 2017). Game theory is significant because most business leaders do not assess the DR plan as the main priority because of funding and time requirements. Game theory can provide a reduction in overall costs by creating efficiencies for resources (Landry & Kroger, 2006). Leaders manage resources strategically to produce the most efficient recovery plan possible.

Logistics management is a strategic requirement at all levels of the manufacturing business. Leaders and managers must understand operational risks to upstream and downstream sustainment technology as a critical strategy to build IT recovery plans against proposed vulnerabilities (Khalili et al., 2017). Business leaders use corporate procedures to maximize use of IT systems to reduce operational lag and unneeded loss of logistic, administrative, production, and communication capabilities during a disaster event (Vanpoucke et al., 2017). Logistics management may have a significant impact on disaster recovery and response effectiveness.

Teams communicate with different individual subject matter experts, internal organization departments, stakeholders, and other sustainment organizations outside the manufacturing business force structure. Leaders use IT communications as a strategic requirement to manage sales, place orders, coordinate upstream and downstream logistic requirements, achieve financial surplus, and keep secure workflow systems operational during a crisis (Argus et al., 2017; Posland et al., 2015). Leadership within an organization work hard to ensure the security of data by protecting against the loss of essential data.

Experts must have the ability to maintain data access through secure systems during a massive disruption to enhance the survivability of an enterprise under duress. For example, managers secure extensive technical data by using cloud orchestration technology to allow teams to back up supporting IT servers, thereby permitting technicians with instant access to lost data during a disaster (Argus et al., 2017). Teams, who develop Internet security strategies for electronics, software, and sensors that can withstand cyberattack, permit managers to maintain operations and will keep the organization healthy against IT disruption (Banerjee & Biswas, 2017). Managers and leaders train their teams to react to specific vulnerabilities within the organization to prevent technology failure.

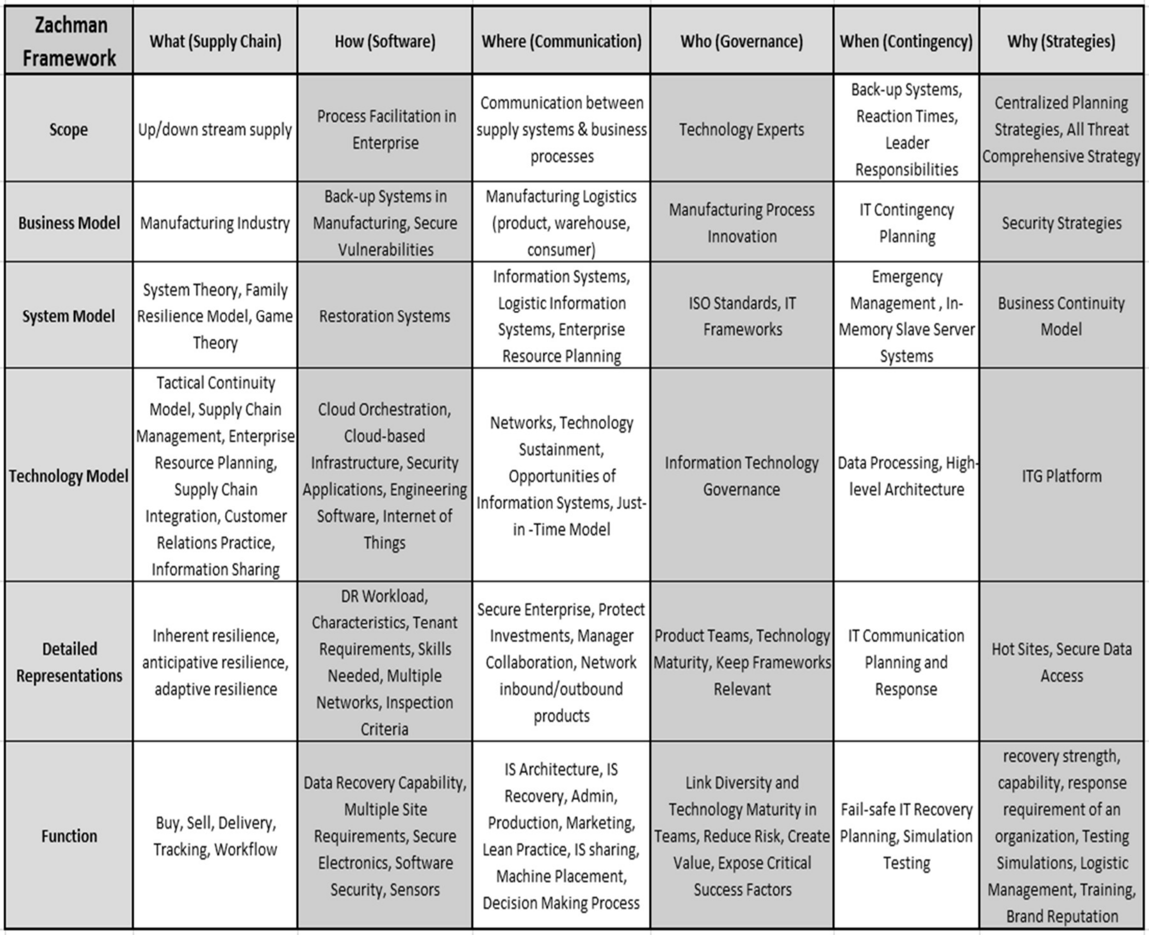
Supervisor led teams confirm manufacture risks and vulnerabilities to test and develop IT recovery plans and IS strategic requirements to strengthen an organization against technical failure during a fabricated or natural disaster. Expert technicians combat risks and vulnerabilities from technological applications in raw material distribution, business infrastructure, and communication technology to provide a foundation for enterprise survivability during a catastrophic episode (Pan, 2017). Teams develop concepts and techniques for IS and IT strategies for organizations, so managers can ensure continuity through all levels of the organization (Cassidy, 2016). Training dedicated leaders, managers, and teams on IT and IS principles will create a more resilient organization when tested by a disaster event.

Stakeholders, leaders, supervisors, managers, and employees should understand that the survival of an organization relies on training. Leaders, managers, and stakeholders fortify their organizations with information systems related to IT recovery planning to achieve business resiliency (Pearlson et al., 2016). Additionally, leaders can use organizational employee behaviors and team cultural norms with IT networks to strengthen the overall IT recovery plan (Almeida et al., 2017). At every level and department, leaders should collaborate to create the IT disaster recovery plan specific to their organizations.

Teams, who collaborate between various levels of management and leadership, will capture more risks and vulnerabilities to an organization compared to one subject matter expert finding gaps in an IT disaster recovery plan. Leaders must develop critical source factors that are relevant to the organization's survivability, while dealing with a disaster event is an essential strategic requirement (Alreemy et al., 2016). Manager can secure organizational needs through employing strategic alignment of leaders, supervisors, employee responsibility, and business opportunity related to IT relationships to protect production against IT disruption (Turel et al., 2017). Leaders, managers, and teams, dedicated to an IT recovery plan, may work long hours; however, if they do not test the projects, then gaps in the project will occur.

Managers of the IT recovery plan conduct "no plan survives contact," simulations, and testing to enhance organizational resiliency and magnify stakeholder awareness. Evidence suggests that managers update plans to reflect test outputs critical for corporate survival (Xu et al., 2015). Leaders and managers face tests that measure their physical, emotional, and technical responses to the IT response plan, which ensures the best response to an IT disruption (Hwang et al., 2016). Managers use team development of IT recovery systems to apply specific technical applications for different types of disruption scenarios. At every level of the organization, leaders should use trusted internal backup systems as strategic applications to uphold performance during a crisis, thereby increasing enterprise survivability, resiliency, and brand reputation (Min et al., 2015). Therefore, leaders use IT strategies for the development of IT disaster recovery plans in the manufacturing industry. Managers can use IT strategies to expand IT recovery processes through the ZFEA theoretical platform and develop the *what, how, where, who, when,* and *why* when coordinating IT disaster recovery plans.

I reviewed professional and academic literature about leaders developing strategic IT recovery planning in the manufacturing industry. Researchers have developed a matrix using the ZFEA EIS application (Lapalme et al., 2016; see Figure 2 for how each area discussed above fits in the ZFEA modal). Leaders use the ZFEA model as a visual guide to capture IT disaster response planning for manufacturing with the understanding that each manufacturing manager will have changes based on geographical location, product, supply chain, and IT systems (Pradhananga, Mutlu, Pokharel, Holguin-Veras, & Seth, 2016). See Figure 2 as an illustration of the ZFEA framework related to strategic IT disaster recovery planning that I have developed based off my literature review.



Zachman Framework	What (Supply Chain)	How (Software)	Where (Communication)	Who (Governance)	When (Contingency)	Why (Strategies)
Scope	Up/down stream supply	Process Facilitation in Enterprise	Communication between supply systems & business processes	Technology Experts	Back-up Systems, Reaction Times, Leader Responsibilities	Centralized Planning Strategies, All Threat Comprehensive Strategy
Business Model	Manufacturing Industry	Back-up Systems in Manufacturing, Secure Vulnerabilities	Manufacturing Logistics (product, warehouse, consumer)	Manufacturing Process Innovation	IT Contingency Planning	Security Strategies
System Model	System Theory, Family Resilience Model, Game Theory	Restoration Systems	Information Systems, Logistic Information Systems, Enterprise Resource Planning	ISO Standards, IT Frameworks	Emergency Management , In-Memory Slave Server Systems	Business Continuity Model
Technology Model	Tactical Continuity Model, Supply Chain Management, Enterprise Resource Planning, Supply Chain Integration, Customer Relations Practice, Information Sharing	Cloud Orchestration, Cloud-based Infrastructure, Security Applications, Engineering Software, Internet of Things	Networks, Technology Sustainment, Opportunities of Information Systems, Just-in -Time Model	Information Technology Governance	Data Processing, High-level Architecture	ITG Platform
Detailed Representations	Inherent resilience, anticipative resilience, adaptive resilience	DR Workload, Characteristics, Tenant Requirements, Skills Needed, Multiple Networks, Inspection Criteria	Secure Enterprise, Protect Investments, Manager Collaboration, Network inbound/outbound products	Product Teams, Technology Maturity, Keep Frameworks Relevant	IT Communication Planning and Response	Hot Sites, Secure Data Access
Function	Buy, Sell, Delivery, Tracking, Workflow	Data Recovery Capability, Multiple Site Requirements, Secure Electronics, Software Security, Sensors	IS Architecture, IS Recovery, Admin, Production, Marketing, Lean Practice, IS sharing, Machine Placement, Decision Making Process	Link Diversity and Technology Maturity in Teams, Reduce Risk, Create Value, Expose Critical Success Factors	Fail-safe IT Recovery Planning, Simulation Testing	recovery strength, capability, response requirement of an organization, Testing Simulations, Logistic Management, Training, Brand Reputation

Figure 2. Illustration of the ZFEA platform related to strategic IT disaster recovery planning. Adapted from "Exploring the future of enterprise architecture: A Zachman perspective," by J. Lapalme, A. Gerber, A. Van der Merwe, J. Zachman, M. D. Vries, & K. Hinkelmann, 2016, *Computers in Industry, 79*, pp. 103-113. Copyright 2016 by Elsevier.

Literature Review Summary

In summary of the literature review, I have expanded upon subjects that possibly fall into required strategic applications within a manufacturing business. The areas reviewed present research related to supply chain networks, manufacturing software, IT network infrastructure, IT governance, IT contingency planning, and IT strategy requirements. I review this research and data collection through the lens of Zachman's enterprise information system frameworks. From my literature review there is a possibility that gaps exist in IT recovery strategies such as IT training, knowledge management (KM) processes, and contingency planning to strategically reconstitute disrupted information systems because of a disaster.

Managers and executives are increasingly becoming concerned with IT disaster recovery efforts, as the cost of downtime and the ability to recover IT systems cost organizations $26 billion in 2010 (Baham, Hirschheim, Calderon, & Kisekka, 2017). According to Baham et al. (2017), a manager needing to recover complex systems during a disaster must understand information system relationships and incorporate a strategic backup plan to successfully recover company IS. Maintenance of IT flexibility during a disaster event and the integration of IS recovery tools and hardware with existing are both essential; however, a knowledge gap presently exists among organizational leaders regarding both (Baham et al., 2017). Training managers to understand IT applications and how teams can use IS recovery tools to ensure manufacturing organizations are free from collapse during a disaster is potentially a strategic gap for IT contingency management. Managers at all levels must be involved in IT decision-making processes in order to strengthen organizational capabilities to withstand disruption and respond to the challenges of innovation. However, to make these types of decisions, a leader must have training. Managers with limited IT training in some business organizations may affect outcomes (i.e., plans) for strategic IT disaster recovery (Ebrahimi & Walsh, 2018). Additionally, proficiency of IT applications is critical among mangers, leaders, teams, and supervisors; this could be another essential gap in strategic IT DR planning.

Knowledge management (KM) from lessons learned and access to worldwide databases of IT DR information are critical. Teams that do not use KM may incur indirect costs associated with a particular disaster, including unwanted visibility to customers, partners, stakeholders, competitors, and credibility concerns of an organization (Mohideen & Dorasamy, 2018). According to Mohideen and Dorasamy, managers using knowledge repositories between client and organizational databases are inconsistent. As the researcher, I present the possibility that a gap exists in KM processes that allow leaders to capture lessons learned data and improve IT DR. Understanding gaps in IT DR will allow managers to provided strategic IT contingency planning during a disaster and will potentially increase the survivability of an organization.

Transition

In this section, I highlighted different technologies for IT recovery planning during a disaster event to maintain business continuity in a manufacturing organization. Additionally, I stated the background of the problem, purpose statement, nature of the study, assumptions, limitations, delimitations, research question, conceptual framework, and a definition of operational terms. Furthermore, I provided a review of the professional and academic literature through the ZFEA framework concerning EIS. In addition, I provided an outline of strategic areas that managers use to plan IT recovery in manufacturing. Areas from the literature review included supply chain network technology, manufacturing software, IT network infrastructure, IT governance, IT contingency planning, and IT strategy requirements. Section 2 is a continuation of the qualitative doctoral study proposal comprised of the purpose statement, my role as a researcher, the participants, research methods and design, population and sampling, ethical research, data collection instrument and technique, data organization technique, analysis, and the reliability and validity of the study. In Section 3, I provide an overview of the research that will include a presentation of findings, application to professional practice, implications to social change, recommendations for action and future research, and a reflection of my experiences conducting this study. Finally, I provide a conclusion at the end to detail findings concerning strategic IT disaster recovery planning in the manufacturing industry and ways in which managers and leaders develop such strategies.

Section 2: The Project

The intent of this study is to discover strategies for planning IT disaster recovery in the manufacturing industry. In this section, I provide a comprehensive review of the methodology and research processes that I use. This section also includes the purpose statement, the role of the researcher, participants, research method and design, population, sampling, and data collection. I also provide a discussion about analysis, reliability, and validity.

Purpose Statement

The purpose of this qualitative multiple case study was to explore effective strategies that some IT managers in the manufacturing industry use to develop IT disaster recovery plans to support business operations. The population consisted of six IT professionals in manufacturing located in the central region of the United States who have knowledge of IT disaster recovery plans. The implications for social change include the potential for manufacturing leaders to gain knowledge of ways in which to develop IT disaster recovery plans that one may use to minimize disruption in the daily lives of consumers and communities during fabricated, terrorist, and natural disasters.

Role of the Researcher

As the researcher, I served as the main device for collection of information. Cooper and Dryden (2016) noted the importance of respecting diversity among participants and instilling awareness of all-consuming truths among researchers. Therefore, I ensured all participant bias, cultural understanding, and ideologies presented were a holistic interpretation of my research and will include my own worldview of the research subject. Additionally, I created a trusted relationship with the participant to empower the contributor (Fleet, Burton, Reeves, & DasGupta, 2016).

As a military business administrator for 28 years, I have basic knowledge of strategic IT disaster response and recovery. However, I had no association with the interview participants within this multiple case study. As summarized in the Belmont report (U.S. Department of Health & Human Services, 1979), researchers must respect participants, diminish risk, and expand the nature of the study. As a researcher, I must respect participants through moral values and procedures to safeguard human themes in research (Fiske & Hauser, 2014). Additionally, I avoided viewing data collected through a personal lens. I maintained strict adherence to the research questions and remained open to feedback from participants, allowing each participant to expand on their own responses during the interviews. Managing and reviewing data with an open mind mitigated personal bias from interrupting the raw data collected. Lastly, I completed the *Protecting Human Subject Research Participants* training offered by the National Institutes of Health (NIH) Office of Extramural Research (Certification Number 2073589) and required by Walden University prior to the conduct of human research. A researcher must review and complete the NIH certification to shield participants from the ethical encounters of research otherwise not known by an untrained researcher.

Participants

Participants were eligible for this study, first, if they had knowledge about the subject matter (Saunders & Townsend, 2016). Since this study involves IT disaster recovery plans, participants I selected came from areas within the manufacturing industry with experience in strategic IT disaster planning and recovery. I assumed participants' knowledge of the subject matter based on their having a current role as an IT professional and previous experience with disaster recovery plans. I included participants in this study who are IT managers, supervisors, organizational leaders involved in IT disaster recovery within different departmental areas (e.g., human resources, operations, and logistics), and team personnel tasked with building strategic IT disaster recovery plans. Each of these categories consisted of IT managers with experience in disaster recovery planning. Participants were eligible for this study if they had at least three years of experience in IT disaster recovery. I perceived three years to be a reasonable amount of time to ensure that the participants are familiar with the strategies for development of IT disaster recovery plans, effectiveness of these strategies, and key obstacles to the implementation of these strategies.

I established a working relationship with participants by first gaining initial access via requests sent through LinkedIn.com to IT leaders within the manufacturing industry located in the central region of the United States who have successfully implemented IT disaster recovery plans. Second, after an IT manufacturing leader has demonstrated his or her interest in the study, I continued the process of establishing a working relationship through scheduling convenient interview times with 6 participants. According to a study by Walsh (2014), it is vital for a researcher to establish a working relationship with the participants to ensure good quality of the interviews. I ensured participant characteristics align with the overarching research question through initial dialogue with the participant. Third, because the research question pertains to IT manager disaster recovery planning, participants consisted of IT managers with experience in disaster recovery strategies. Fourth, I ensured that I adhered to federal regulations concerning human research, IRB policies, and employee vulnerabilities, in accordance with recommendations from previous research (Resnik, 2016). Lastly, I ensured the privacy and confidentiality of all participants and further provided potential candidates with study information ahead of requesting an interview. This was geared towards ensuring the participants were able to make an informed decision regarding whether to participate in the study.

Research Method and Design

Research Method

I selected a qualitative, multiple case study approach for my research. According to Colorafi and Evans (2016), qualitative methodologists create results from thoughtful investigation of intricate issues. Qualitative methods include a variety of philosophical styles and methods that researchers use to acquire a detailed understanding or clarification of participants' insights on a given subject (Vass, Rigby, & Payne, 2017).

Researchers have used qualitative approaches to gain an understanding of different perspectives, learn unexpected findings through participants, and use peer-reviewed material to access relevant information (Vandermause et al., 2017). Researchers have used the qualitative method to expand their understandings of basic human phenomena on a given subject. Qualitative researchers achieve data saturation to reveal unforeseen responses to human nature through expert participants and their practices within the purpose of the research (Vandermause et al, 2017). The qualitative research method is most appropriate for this study because I expanded on current practice by exploring the expert knowledge of professionals aligned with IT disaster recovery plans and strategies.

Researchers use quantitative methods to translate data numerically and examine differences in variables to test a hypothesis (Patten & Newhart, 2017). A quantitative method is not suitable for this study because I did not examine relationships between variables or testing hypotheses. Researchers use a mixed method approach to combine qualitative and quantitative methods in a study, and then triangulate among the associated variables (Turner et al., 2015). A mixed method approach was not suitable for this multiple case study because I did not use a quantitative method to explore a given subject. Thus, I selected a qualitative method, specifically using a multiple case study design, to produce a rich description of IT managers' IT disaster recovery strategies in the manufacturing industry.

Research Design

I selected a multiple case study design for this study. Four possible qualitative study designs include narrative, ethnographic, phenomenological, and grounded theory. Each of these designs is specific to the type of research conducted by the researcher. Researchers use case study to examine an in-depth, real-life phenomenon within a specific framework derived from participant interviews, previously recorded information, and observations to find patterns and associations that affect an event (Ridder, 2017). Through the multiple case study design, I explored strategies used by IT managers in the manufacturing industry to enhance IT disaster recovery plans.

A narrative researcher explores complexities of the human experience regarding an individual story or nuances of a personal experience (Nolan, Hendricks, Williamson, & Ferguson, 2018). Participants provided a narrative study that consists of their experiences of a phenomenon under study. I did not select a narrative design because I did not explore a personal experience, nor gather written narratives. Rather, I learned through interviews ways in which leaders and managers use frameworks to create specific strategies for IT disaster response in a manufacturing business.

Ethnographic researchers emphasize detailed observational evidence pertaining to a particular culture and related historical events in a natural setting (Yin, 2017). A researcher uses an ethnographic design to process information on a given culture for an extensive time to ensure a correct sample with specific parameters about a population (Bernard, 2017). Ethnographic design was not appropriate for this study because I explored strategies managers use for IT disaster recovery and not a specific culture.

Researchers use a phenomenological design to detail research specifically based on participants' lived experiences (Lewis, 2015). A researcher can use a phenomenological design to understand lived occurrences as depicted within a knowledge base of a specific phenomenon (Thompson, Grocke, & Dileo, 2017). A phenomenological design was not appropriate because I explored participants' strategies for IT disaster recovery plans and not lived experiences about a specific phenomenon.

A researcher uses a grounded theory design for theoretical sampling to formulate new theories based on first-hand data in the development of a social process from the field (Glaser, 2017). Because I did not develop a theory within my research or evaluate a social process or action, grounded theory design was not suitable for this study. I used a multiple case study design to explore the patterns and associations that leaders use to develop strategies for IT disaster response plans.

As the researcher, I ensured data saturation through constant review of electronic resources, participant interviews, and information tracking through the data collection process. Data saturation occurs when there is enough evidence that the researcher begins to find only repeated information (Walker, 2012). In this study, I achieved data saturation through the interview questions during data collection. According to Kwong et al. (2014), researchers using the qualitative method will reach data saturation through the interviewing of participants. I asked follow-up questions when needed during the interview. I interviewed the participants and only stopped when data saturation occurred. A saturation point happens when there is sufficient data to ensure that the research question(s) reach full data collection potential (Bernard, 2017). I determined saturation subjectively upon collecting data, based on the observation that no new explanations or perspectives are present concerning the research question. Additionally, as a qualitative researcher, I ceased interviewing when participants could no longer produce new information on my research topic (Bristowe et al., 2014). Lastly, I constructed a saturation grid when collecting data in order to list all major themes and topics that emerged. When I no longer could expand on themes or topics generated from participants, I inferred saturation and began data analysis.

Population and Sampling

I used purposeful sampling for my research study. Hoeber, Hoeber, Snelgrove, and Wood (2017) noted that purposeful sampling is a data reduction style for qualitative study based on participants and their specific relevance of the topic. A researcher uses purposeful sampling to maximize information about a specific phenomenon based on the experiences of the participants (Hayes, Wolf, Labbé, Peterson, & Murray, 2017). When using purposeful sampling as the data collection method, researchers select individuals or groups based on their knowledge regarding the subject of study (Mufti, Ahmad, & Khan, 2018). According to Sarstedt, Bengart, Shaltoni, and Lehmann (2017), researchers who employ purposeful sampling must use their best judgment or expertise to select participants who are appropriate for providing information for the research study. A researcher uses purposeful sampling to ensure appropriate data collection for the conduct of rigorous and complex studies (Gerassi, Edmond, & Nichols, 2017). I used purposeful sampling to achieve my sample of six IT professionals.

Participants in this study provided clarity and confirmed themes within the research study. Researchers must determine correct sample size to provide certainty in conclusions sited within the study (Lane & Hennes, 2018). Guest, Namey, and McKenna (2017) suggested that 16 participant interviews are enough to discover additional themes after data saturation. However, researchers use 20 to 40 interviews to identify meta-themes across an organization and achieve data saturation (Guest et al., 2017). According to Orser, Eliott and Leck (2011), data saturation confirms emerging themes through expansion of participant interviews. Researchers use two styles when selecting sample size: desired effect and estimation of how large the effect is likely to be (Anderson, Kelley, & Maxwell, 2017). For my qualitative study, and due to the low density of IT professionals within manufacturing industry, I conducted 6 interviews with IT professionals within the central U.S. manufacturing industry in order to identify meta-themes. The interview setting was in a private location so that the participants were more comfortable to share their opinions and experiences (Marshall & Rossman, 2016).

The intended sample included IT professionals, leaders, managers, and subject matter experts within a manufacturing organization located in the central United States. Specifically, I recruited IT professionals within the manufacturing industry from across all functional areas available. At all departments of the organization, IT professionals handle productivity, competitiveness, efficiency, decision making, optimization, operational risk reduction, improved product, service delivery, and resilient disaster infrastructure and capabilities (Papadopoulos et al., 2017). I ensured data saturation by selecting experts in the IT industry who are familiar and experienced with the phenomenon under study—strategies used within IT recovery plans.

Ethical Research

When I received Institutional Research Board (IRB) approval, I invited participants selected from the manufacturing industry in the central United States to participate in my qualitative, multiple case study research project; ethical research is the highest priority. During the participant recruitment process, I focused on strict ethical requirements set by Walden University officials, U.S. federal regulation, and applicable international guidelines. One of the incentives for the participants' input in the research was to aid in establishing any current gaps in the study and help in identifying areas for future studies on the same. Additionally, I illustrated ethical research criteria through a consent form that included the purpose of the study, my role as a researcher, participant withdrawal procedures during the ongoing study, disclosure motivations, data protection requirements, and intent of research findings. According to Nishimura et al. (2013), ensuring documented participant consent is a mandatory requirement when conducting research. Using the Walden University IRB process, I ensured I upheld ethical principles to maximize benefits and minimize harms. In addition, I evenly distributed research documents and protected the participants and their organizations. The Walden IRB approval number for this study is 02-05-19-0641720.

When conducting any kind of research, researchers require informed participant consent (Sembajwe & Kunwar, 2016). Researchers use consent forms to ensure ethical practice for participants and their organizations. According to Walton (2016), researchers cannot issue misleading or partial information to participants who voluntarily agree to take part in research projects. The researcher must receive training and education required to ensure he or she communicates written participant rights to participants within the consent form in areas of anonymity, confidentiality, and nonaffected participant withdraw (Wilson, Kenney, & Dickson, 2018).

Confidentiality of participants in human research and the organization in which they work is a strict requirement. Researchers use an informed consent process to uphold the ethical demands of any research project and define the nature of the study in relatable terms (Sil & Das, 2017). In this study, I concealed the names of the individuals or organizations, using unique identifiers (e.g., Participant 1, Organization 1) to refer to participants or organizations. I also communicated the knowledge that participants may withdraw at any time during the study with no effect to the participant. Finally, I stored documents and data collected in this study for the next five years, while keeping names and organizations confidential.

Data Collection Instruments

I used a semistructured interview protocol (see Appendix A) as the primary data collection instrument. Semi structured interviews are similar to a guided conversation, with fluid questions, rather than structured questions. The researcher uses semi structured interview to allow participants to expand on facts, as well as their opinions; interviewees also interjected their own insights as the basis for further inquiry (Given, 2008; Yin, 2017).

As the researcher, I ensured information collection methods enhanced the reliability and validity of the data; starting with the interview protocol. Researchers use interviews as an essential data source within case study design (Yin, 2017). I used an interview protocol to maintain a consistent line of inquiry and guide the interview. The protocol includes open-ended questions, which I related to the research questions to yield in-depth responses about participants' experiences, perceptions, opinions, feelings, and knowledge, as suggested by Patten (2002). Additionally, I combined the member checking technique after each interview to further incorporate validity between the participant and myself. Member checking produced successful knowledge exchanges throughout the interview process to ensure the exchange of information matches the data received from the participant (Madill & Sullivan, 2017). The member checking technique in combination with the interview protocols were essential instruments in the data collection process.

I have developed the interview protocol to consist of six questions based on existing literature on IT disaster recovery plans that I used to address the research questions. To assure trustworthiness, credibility, dependability, and clarity, I conducted a field test of the interview questions with one IT professional who had experience on the proposed topic; however, the IT professional did not participate in the actual study. Given (2008) observed that researchers can use field tests to assess flaws, limitations, or other weakness within the interview design. I used the field test approach in order to identify any necessary revisions to the interview protocol required before I conducted the study.

I conducted document reviews as the second data source. Researchers use document reviews to acquire relevant data to support data collected from participants, provide additional data not referred to by participants, and show potential changes on the topic of study (Bowen, 2009). I used a checklist (see Appendix B) of items specific to IT disaster recovery plans to categorize common themes associated with data collection and presented during the interviews. The checklist ensured no bias exists during the review of and processes expanded upon by the participant only, and I only collected data related to the subject under study and only in areas the participants discussed.

Data Collection Technique

I collected data from semistructured interviews with six IT professionals of the manufacturing industry located in central United States. I asked IT professionals to participate in an interview session to collect their perceptions of effective strategies used within IT disaster recovery plans. I conducted the interviews in a comfortable and relaxed atmosphere of the participant's choice, where the participant felt free to give their opinions and ideas regarding the study subject. I conducted each interview at a convenient time and place to ensure the participant is comfortable during data collection. I estimated that each interview was 30 minutes to an hour.

Pilot studies are a useful tool for scholars to commit extensive resources to a larger study; however, one must use caution with pilot studies as to not allow early opinions to persuade final outcomes. According to Rachel, Laura-Mae, Barbara, and Donna (2018), when conducting qualitative research, pilot studies can have an adverse effect because researchers will draw conclusions from incomplete data. While pilot studies are a useful instrument that allows researchers to test methodology, effectiveness of data collection, and analysis prior to a more expansive study, pilot studies also give research teams the ability to expose large-scale investment criteria for financial requirements and may take six to twelve months to complete prior to the main study (Henson & Jeffrey, 2016). While pilot studies are a useful tool, a researcher's inquiry of this magnitude may obligate unneeded resources.

Another term used to describe a pilot study is the feasibility study. That is, a feasibility review to use certain protocols for data collection, processes, and unforeseen statistical data needed to test research requirements (Dahlia, Togar, & Priyantono, 2018). Researchers conducting large-scale studies with assigns staffs and budgetary requirements will often execute a pilot study (i.e., feasibility study) prior to allocating human and finical requirements to a research project. Because I was the single researcher without budgetary requirements, and because the need to complete this study in a timeframe conducive to sourcing requirements, a pilot study could have created unneeded time constraints. Additionally, when reviewing strategies IT managers use in manufacturing for IT disaster recovery, it is important to avoid creating bias through a pilot study that could affect outcomes generated from participants. Lastly, there was a need to understand technical response capabilities in business within natural disaster events, or manmade crisis; as the researcher, a full-scale research project allowed me to identify these strategies upfront without a pilot study requirement. Because there is enough research to validate the need for information concerning strategic IT DR processes, I did not conduct a pilot study after IRB approval.

Face-to-face interviews have advantages and disadvantages. One of the disadvantages is that it can be too time-consuming (Marshall & Rossman, 2016). On the other hand, interviews are effective tools in obtaining detailed data about the experiences of the participants (Marshall & Rossman, 2016). Interviewing subject matter experts is a critical construct to the outcomes and deliberations of the overall project.

I guided each interview using an interview protocol (see Appendix A). An interview protocol is an instrument of inquiry to ensure that the interview questions are at per with the aims of the study (Patton, 2015). I used an audio-recorder to ensure I capture participant responses verbatim with sufficient context to be interpretable, as suggested by Patten (2002). I then transcribed audio recordings into a Microsoft Word document and save each under a pseudonym. I sent transcripts via email to respective participants and asked each participant to review their transcript to ensure I captured responses accurately. I used member checking of data in order to improve the reliability and credibility of the analysis. Member checking is a technique used during the interview process where the research reiterates and summarizes what the participant has said, to include allowing participants the opportunity to critically evaluate findings (Bernard, 2017). Within my study, I performed member checking following each interview and require a confirmation of the completeness of data from each participant to ensure I had interpreted all data correctly and that data is both accurate and authentic.

I also requested organizational documents from participants by collecting recovery plans, training materials, policies, procedures, and reports, at a time convenient for participants. I used a document review checklist to identify collected documents protocols and outcomes related to IT disaster recovery. After conducting a review with each document acquired, I contacted participants for follow-up questions to gather sufficient data on strategies previously or currently used for effective IT disaster recovery plans.

Data Organization Technique

Data consisted of transcribed interviews. I transcribed interviews into a Word document from audio-recordings after each interview following the established qualitative methods (Mishra et al., 2018). In regard to keeping track of data, I labeled each transcript with a pseudonym, which I stored on a flash drive. I entered document review checklists into an Excel spreadsheet, with each labeled under a code and date related to the document. For example, I identified reports as R1_xx/xx, R2_xx/xx in order to keep track of data (Hopf, 2014). In addition, I stored the spreadsheet on an encrypted flash drive to prevent tampering or unauthorized access and will destroy all data after five years. All decisions made concerning data organization are in accordance with guidance from recent research and texts on qualitative methods (Bernard, 2017; Colorafi & Evans, 2016). According to Bernard (2017), three note-taking techniques are available to help researchers organize qualitative data: (a) *scratch notes* (e.g., quick memory notes), (b) *diary notes* (e.g., main ideas that form the study), and (c) *logs* which allow researchers to schedule different subjects to catalog and enter into writings about the study. As the researcher, I used all three techniques to gather required information. I used the Microsoft product OneNote as my primary note-gathering application. I used Bernard's note-taking techniques and OneNote to ensure that I keep data organized and coded appropriately.

Additionally, Colorafi and Evans (2016) observed that data representation techniques allow researchers to define results clearly. Colorafi and Evans identified the following three techniques for collection of qualitative data: *conventional content analysis* (e.g., data collected from open-ended questions and recorded word for word by participants), (b) *directed content analysis* (e.g., coding theories and research data), and (c) *summative content analysis* (e.g., sorted into electronic word searches that are applicable to the research subject. Using the aforementioned data collection methods, I applied *conventional content analysis* to my participant interviews using open-ended questions to allow the participant unconstrained expansive conversation. As the researcher, I used directed content and summative content analysis derived from note taking techniques to create an organized, electronic matrix of information derived by my conclusions from section three of my study.

I kept all audio recordings under a password-protected file on a password-protected computer in accordance to the data security measures and procedures described in a study by O’Toole, Feeney, Heard & Naimpally (2018). I stored both flash drive and computer in a locked cabinet within my office. I kept informed consent forms in an unmarked envelope stored separately within the locked cabinet. I am the only individual with access to the locked cabinet. I will store data for five years, at which time I delete all electronic data and shred any hard copies of data.

Data Analysis

Data analysis is a critical event to fully triangulate data from other points of view and to fully integrate data into information outcomes delivered from the interview process. As the researcher, I used triangulation to complement rather than compete with different data outputs (Abdalla, Oliveira, Azevedo, & Gonzalez, 2018). Observations by Abdalla et al. (2018) suggest *data triangulation* provides different points of view concerning validity and reliability of research by using more than one source of data such as interviews, questionnaires, observation, and field notes. Additionally, I used Braun and Clarke’s (2006) six-step process for thematic analysis to analyze interview transcripts and data collected from the document review. I analyzed each transcript and document according to the following six steps: (a) familiarize one’s self with the data, (b) generate initial codes, (c) search for themes, (f) review themes, (e) define and name themes, and

(f) produce the report. I used the process to determine themes related to the research questions and purpose of the study.

Per Braun and Clark's (2006) process, the first step in any qualitative analysis involves reading and rereading the transcripts. I conducted the same review of the document review checklist. In addition, I used NVivo, qualitative analysis computer software, to assist with the data analysis procedure (Castleberry et al., 2014). In the next step, I generated initial codes and organize data in a meaningful and systematic way. I use coding to reduce the large amount of data into small units of meaning (Perrin, 2001). I then conducted a search for themes. I characterized a theme by its significance and relevance to the study topic and the guided research questions. I fit codes clearly into a theme or set these aside for the next step that required me to review themes. During this fourth step, I reviewed themes for modifying or in developing new themes. Once I determined themes as appropriate according to the research question and purpose of the study, I created definitions for themes. Lastly, I presented themes and supporting data.

Reliability and Validity

Reliability

One of the major concerns of any study is to maintain reliability and trustworthiness throughout the research process. Researchers who must facilitate reliability in qualitative research can face underlying concerns associated with producing results that other researchers can replicate using the same procedure (Merriam, 2009). Merriam (2009) identified several strategies in describing the reliability and dependability of qualitative research: (a) use clear research questions, (b) describe the researcher's role explicitly, (c) generate findings from meaningful parallel data sources, (d) connect reliability to theory, (e) collect broad data, (f) perform data checks, and (g) use peer review.

To ensure dependability, I utilized member checking in accordance with recent peer-reviewed guidance on qualitative research methods (Bernard, 2017; Colorafi & Evans, 2016). I reviewed all interview transcripts with participants at the conclusion of each interview to allow for critical evaluation and to ensure accuracy, authenticity, and completeness (Ang, Embi & Yunus, 2016). To ensure reliability, I conducted transcript review. Transcript review is used to ensure transcriptions are an accurate representation of participants' words and to allow participants to expand on their responses if desired (Given, 2008). I also collected data from multiple sources, including semistructured interviews and document reviews, and I explicitly described my role to the interview respondents (Sechelski & Onwuegbuzie, 2019). The reliability of the participants is crucial to the study. I triangulated every comment made by participants with inputs from other sources to evaluate the accuracy of the statement.

Validity

Patten (2002) noted the utility of data triangulation strategies in establishing validity in qualitative research. Patten (2002) noted that triangulation of data sources was a time- and cost-effective strategy to ensure validity of study findings. I achieved triangulation by reviewing transcripts, employing member checking of transcripts, and using a document checklist to confirm data collected.

Qualitative validity strategies include peer review and debriefing, member checking (i.e., consulting with the participants for feedback after completed results), and external audits (Lincoln & Guba, 1985; Merriam, 2009). Researchers use member checking to support credibility in a qualitative study and provide a foundation of overall trustworthiness of the research findings; participants will validate the accuracy of their responses to determine any misrepresentation present in the data (Merriam, 2009). In this study, I conducted member checking to support the validity of my research data.

Merriam (2009) observed successful transferability and fittingness of validity requirements when (a) researchers use information-rich thick descriptions for readers, (b) findings are consistent with experiences of participants, (c) the study supports further testing, and (d) other researchers can replicate the study. To address transferability, I provided detailed description of the data collection and data analysis procedures conscientiously followed them. To enhance confirmability, I documented the checking and rechecking of data. According to Lincoln and Guba (1985) regular audits of information collected from participants and all sources enhance the ability of the researcher to review and analyze data for potential bias and strengthen the validity of the research.

Data saturation is a measurement to ensure that data collected is adequate and of high quality (Walker, 2012). I ensured data saturation through the recruitment of the participants. When I reached data saturation before the last participant, I stopped data collection. When I did not reach data saturation after the last interview, I recruited more participants.

Transition and Summary

The purpose of this qualitative multiple case study is to explore strategies that some IT managers in the manufacturing industry use to develop IT disaster recovery plans to support business operations. The targeted population will consist of ten IT managers in the manufacturing industry located in the central region of the United States who have successfully implemented IT disaster recovery plans. I conducted semistructured interviews and a document review to learn of effective strategies implemented within IT disaster recovery plans. I used Braun et al.'s (2014) six-step process for thematic analysis to analyze interview transcripts and data collected from the document review.

In Section 3, I discuss study findings, application to professional practice, implications for social change, recommendations for action and future research, and a reflection of my experiences conducting this study. I based my conclusions in Section 3 on the research outcomes that suggest gaps in the strategic planning process for IT DR in manufacturing organizations. I documented a detailed account of observations through the data collection processes, which teams, managers, leaders, and supervisors for the development of IT DR plans.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore effective strategies that some IT managers in the manufacturing industry use to develop IT disaster recovery (DR) plans to support business operations. I sourced six subject matter experts (SME) from the Central United States who had extensive planning backgrounds in IT DR concerning manufacturing organizations, IT continuity planning, and knowledge of offsite technology centers. All consenting SME participants had either direct or indirect experience with manufacturing, offering an aggregate of over 90 years of IT DR planning service. Individuals who agreed to participate within this study provided responses that addressed the overarching research question and assisted in the discovery of strategic themes within the data gathered. Participants responded to several strategic nodes in IT DR such as: (a) defining human factors, (b) testing and updating IT DR, (c) understanding threats, (d) knowing time responses after disruption, (e) cost associations, and (f) levels of IT DR requirements. All the SME participants interviewed indicated that while IT DR plans differ in the type of disaster and location, there are specific areas to focus on from a strategic perspective in order to maintain continuity with business operations. The main themes that surfaced through the collected participant data were: (a) contingency planning by priority within in a given IT network, (b) testing plans for natural disasters, advisory attacks, and human errors, (c) network locations and levels of response by crisis, (d) understanding time requirements for recovery by organization, and (e) costs associated with having a strategic IT DR plan.

Presentation of the Findings

The overarching research question for this study was: What effective strategies do some IT managers in the manufacturing industry use to develop IT disaster recovery plans to support business operations? The participants were identified using the following codes: P1, P2, P3, P4, P5, and P6. I developed semistructured interviews and open-ended questions to collect data from participants with digital recording of each interview when the participant granted permission. I placed this recorded data into a qualitative software tool referred to as the NVivo application in order to observe the "what, how, where, when, and why" aspects of the Zachman (1987) framework applied to my study. I identified strategic themes based on participant interviews that align to Zackman's framework in identifying the what, how, where, when and why aspects of the data, as indicated below: (a) determining the 'what' in terms of contingency planning by priority within a given IT network, (b) establishing the 'how' when it comes to testing plans for both natural disaster, advisory attack, and human error, (c) planning the 'where' with regards to network locations and levels of response by crisis, (d) ascertaining the 'when' in terms of understanding time requirements for recovery by organization, and (e) establishing the 'why' in relation to the costs associated with having a strategic IT DR plan.

Theme 1: Contingency Planning by Priority (What)

When recovery time of IT DR is of the essence, contingency planning by priority may be the answer. Uddin, Hapugoda, and Hindu (2015), define technology disaster as actions that cause harm to IT applications in a prime site used by the total organization day-to-day and could render the daily output useless. Under this premise, all participants in this study agreed that while planning recovery for a prime location is fundamental, one must also plan for priority contingencies for IT applications within the prime site, or sites, in order to meet recovery time objectives (RTO). For example, P5 alluded to RTO for his organization to be only two hours in any location; that is, the IT applications disrupted must be back online and operational within two hours after a disaster in order to keep production seamless. As such, P5 posits that in order to meet this time requirement IT applications by priority are the immediate response to the IT DR plan. Table 1 below illustrates the frequency participants referenced prioritizing contingency planning by critical systems as a key strategic development.

Table 1

Frequency of Strategic Need to Prioritize Contingency Planning (What)

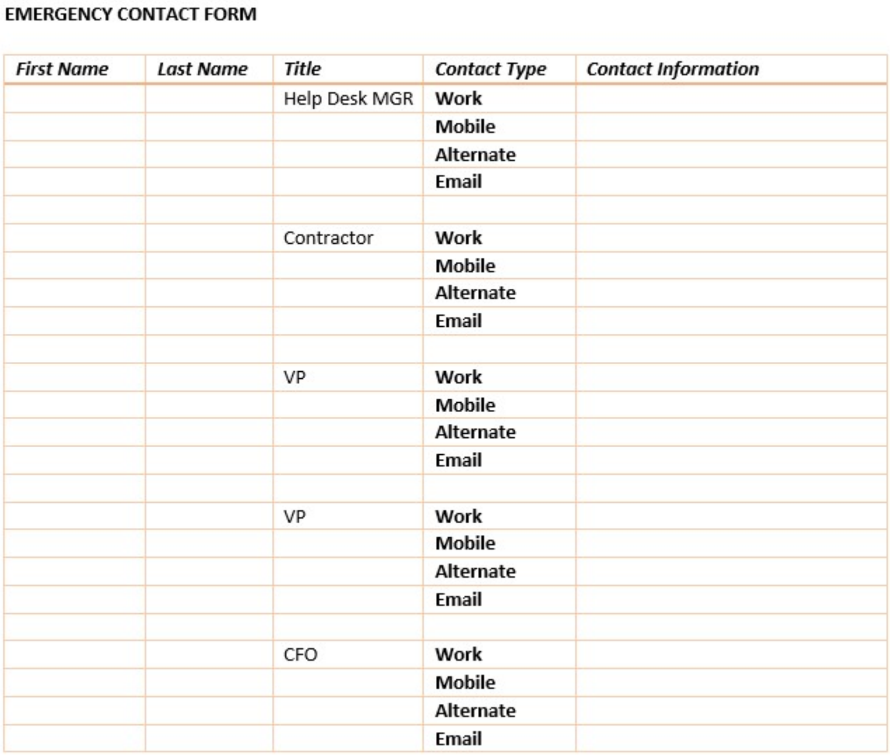
Participant	Interview questions	Total number of references
P1 (M)	1,4,5	6
P2 (D)	5	1
P3 (D)	1	2
P4 (M)	1,2,3,4	8
P5 (M)	2,6	2
P6 (C)	1,2,3,4	6

Note. Participants with “M” represent employment at a manufacturing organization. Participants with “D” represent a Department of Defense employment that relate to systems in manufacturing. Participants with “C” represent outsource continuity planners that work with several large-scale manufacturing organizations.

Priority systems selected for the most time sensitive response differ by type of disaster, size of organization (e.g. multinational corporation; small, medium, large), and costs associated with requirements. P6 stated, “Know what kind of disaster it is that you will plan for.” P5 also noted that if a disaster occurs such as a fire, tornado, or flood, replication of data between as many as three off site data centers at different geographic locations might be needed depending on the size of the organization in order to create resiliency against the IT disruption and use of priority systems. For example, P6 noted, “It’s about the human element and not just technology…who is the first person that needs to know about the disaster.” Such as using a call tree as part of a strategic plan during the crisis fosters the correct prioritization of communications.

IT communication systems are strategic resulting from notification efforts to employees at all levels of management, functionalities (e.g., HR, operations, logistics), and locations. Without a strategically developed commination design within the IT DR plan, the disaster recovery asset fails immediately because there is no message to activate people, assets, IT applications, contingencies, and resources within the plan.

Additionally, secondary efforts once communications are re-established, could be notification to suppliers that deliver or transport materials to the manufacturing location and IT systems that manage product distribution within supply chain operations. Figure 3 is an example emergency contact form developed by P1 in relation to the use of the physical communication tree as a strategic requirement to action a contingency plan (organization, names, and contact numbers removed). While this is the simplest way to convey a communication plan, there could be another automatic action in place to activate IT DR plans. For example, if an earthquake hits the western region of the United States where a manufacturer is located, perhaps the central region of the U.S. where contingency assets for the same organization are located react immediately to the event without a formal request from the affected area.



EMERGENCY CONTACT FORM

First Name	*Last Name*	*Title*	*Contact Type*	*Contact Information*
		Help Desk MGR	**Work**	
			Mobile	
			Alternate	
			Email	
		Contractor	**Work**	
			Mobile	
			Alternate	
			Email	
		VP	**Work**	
			Mobile	
			Alternate	
			Email	
		VP	**Work**	
			Mobile	
			Alternate	
			Email	
		CFO	**Work**	
			Mobile	
			Alternate	
			Email	

Figure 3. Illustration of the Emergency Contact Form used developed by participant one for IT DR planning.

As mentioned in my literature review (Section 1), (a) inherent resilience (system strengths), (b) anticipative resilience (preparatory capabilities), and (c) adaptive resilience (coping) are three resiliency traits incorporated into IT response and recovery plans concerning supply chain operations (Azadegan and Jayaram, 2017). While all participants agreed on recovery as containing multiple back-up systems, P3 indicated that their multiple back-up sites used off site or cloud technology, or other physical locations away from the anticipated disaster location to ensure system recovery resiliency concerning strength, adaptability, and preparations of strategic IT DR plans. Lastly, the tertiary effects after communication and supply chain operations are reconfigured, may be systems that activate alternate off-site production assigned as a backup location known as hot, cold, and warm sites. While all participants agreed that contingency planning within all business functions of the IT DR are critical for organizational survival, the manufacturing industry had more specific contingencies concerning supply chain management.

> P6 observed, Predestined locations were established for warehousing products at a separate location, where trucks would back up to the affected area and move the products to the unaffected site, this was practiced but when an actual flood occurred 50% of personnel that actioned the plan were affected, and the plan failed immediately.(P6, personal communication, May 30, 2019)

If a catastrophic event occurs, disruption of a critical supplier or products will affect production within the manufacturing process. In order to minimize this risk of material or product shortages, manufacturing firms will order resources from a competitor supplier and warehouse outside a possible affected area and establish wholly owned subsidiaries that produce the resource in multiple locations that can be easily diverted if one supplier is disrupted (Sawik, 2017). While the aforementioned describes aspects of the contingency plan within a SC, all participants agreed that IT communication affects supply chain continuity and communication resiliency and is a key construct to back up during any disaster event. Simply put, the contingency plan for a supply chain disruption does not happen without IT DR planners redirecting supply assets from a technical transaction (i.e., communication) to the supplier.

According to the views of the present participants, data loss in any system application, and the recovery of that data, form part of the crucial effort for the IT DR planning process. In some cases, participants revealed that manufacturing organizations might require 100% of all systems, regardless of priority, to recover simultaneously. According to P1, P3, and P6, this requires different levels of remote recovery technology configurations referred to as mirror site, hot site, warm site, and cold site configurations and defined in more detail below and later under *location requirements* within this study.

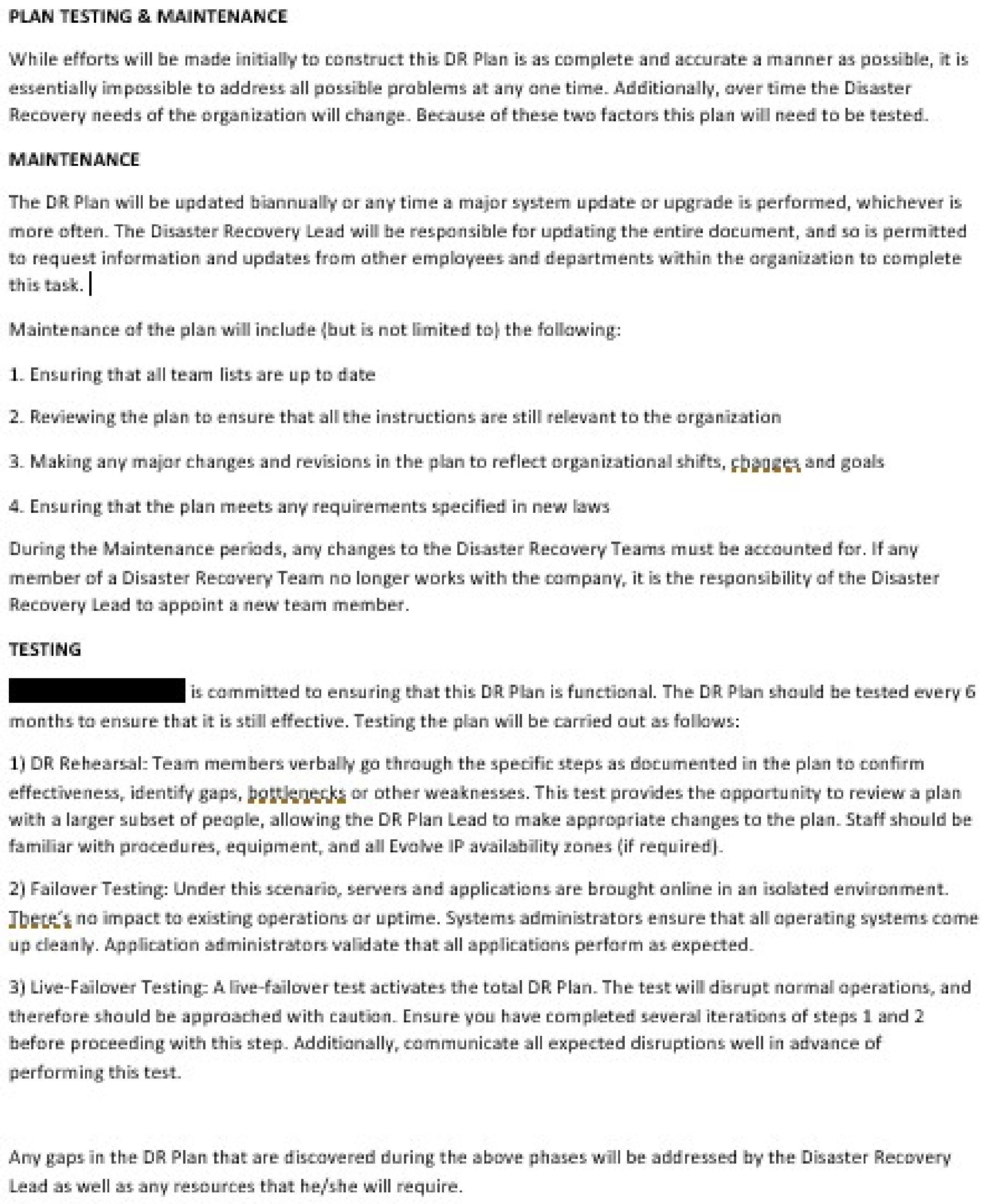
A mirror site refers to a disaster recovery back up site that has been rendered redundant but one that contains real time information that is identical to a company's or an organization's primary site. Compared to the other backup sites, a mirror site offers the fastest recovery time for the organization following a disaster (California Judicial Branch, n.d). A hot site in this context refers to a continually operating backup site that enables an organization or company to resume its normal business operations within a very short time following a disaster. Characteristically, the hot site is online and must be equipped with all the necessary software, configurations, software, and internet connectivity. A warm site is also a backup site but one that lacks in equipment compared to the hot site. As such, by using a warm site, the organization takes a relatively longer period before being fully operational. A warm site is equipped with servers and configured with a network. The cold site is also a backup site that is characterized by fewer configurations and equipment compared to the warm site. As such, through the cold site, it takes an organization a relatively longer period before resuming operations (CISSP CIB, 2012).

When constructing an IT DR plan, it is critical to address systems that IT managers must recover from disaster events that would otherwise bring production to a halt. Every organization has unique characteristics that require leaders to develop more than just one single disaster recovery solution (Mendonça, Andrade, Endo, & Lima, 2019). For example, according to participants, a cold site represents the lowest level of recovery and used for a larger RTO requirement with perhaps a lower budget for IT DR. In participant two's view, "a cold site would represent a separate geographical location that has the capacity to recover all organizational data, but is not staffed and only has the capacity to store and recover data at the time of the disaster." According to participants, a hot site is a top-level recovery asset because it can be used as an alternate location that supports all production. The hot site would include manning and infrastructure allowing seamless recovery when the network systems cease to work because of a disaster event. According to all participants, leaders use multiple IT recovery options in one IT DR plan such as cloud technology, hot and cold sites with data recovery systems, and production recovery assets according to RTO and cost requirements. Once IT DR platforms are in place, IT managers further develop and expand IT recovery platforms through testing as another strategic advance of IT DR planning.

Theme 2: Testing Plans (How)

Through my many years in the military environment, I have deduced that no plan is perfect. As the researcher, there are several areas within an IT DR plan for manufacturing that I feel require testing. These factors include production software, cloud-based infrastructure, IT security, Internet-of-Things (IOT), and engineering software. According to all participants, testing an IT DR strategy requires a critical understanding of the strengths and weakness within the plan and then continued updates to ensure the plan is solid. P2 noted, “The main obstacle within an IT DR plan is time to conduct actual testing of the plan during business. Whether using hot or cold sites, an unpracticed IT DR plan in any critical area is possibly more dangerous than not having one at all” (Edwards & Cooper, 1995).

While cost and time are major planning factors in most manufacturing organizations, frequency of testing matters. One hundred percent of all participants interviewed in this study mention testing as a strategic planning factor; more importantly, updating the IT DR plan after the test occurs in order to close gaps and increase the credibility of the plan. Testing and updating plans are critical and curtailed to fit each organization specific risk assessment needs within a geographic location (e.g., flood, earthquake, fire, cyber-attack). See Figure 4 below as an illustration of testing requirements within an IT DR plan. While time and money are the concern, the cost associated with a disaster event causing a disruption in manufacturing is devastating.



PLAN TESTING & MAINTENANCE

While efforts will be made initially to construct this DR Plan is as complete and accurate a manner as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the organization will change. Because of these two factors this plan will need to be tested.

MAINTENANCE

The DR Plan will be updated biannually or any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery Lead will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization to complete this task.

Maintenance of the plan will include (but is not limited to) the following:

1. Ensuring that all team lists are up to date

2. Reviewing the plan to ensure that all the instructions are still relevant to the organization

3. Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals

4. Ensuring that the plan meets any requirements specified in new laws

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the company, it is the responsibility of the Disaster Recovery Lead to appoint a new team member.

TESTING

[redacted] is committed to ensuring that this DR Plan is functional. The DR Plan should be tested every 6 months to ensure that it is still effective. Testing the plan will be carried out as follows:

1) DR Rehearsal: Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the DR Plan Lead to make appropriate changes to the plan. Staff should be familiar with procedures, equipment, and all Evolve IP availability zones (if required).

2) Failover Testing: Under this scenario, servers and applications are brought online in an isolated environment. There's no impact to existing operations or uptime. Systems administrators ensure that all operating systems come up cleanly. Application administrators validate that all applications perform as expected.

3) Live-Failover Testing: A live-failover test activates the total DR Plan. The test will disrupt normal operations, and therefore should be approached with caution. Ensure you have completed several iterations of steps 1 and 2 before proceeding with this step. Additionally, communicate all expected disruptions well in advance of performing this test.

Any gaps in the DR Plan that are discovered during the above phases will be addressed by the Disaster Recovery Lead as well as any resources that he/she will require.

Figure 4. Illustration of written policy concerning test requirements within an IT DR plan.

All participants agreed that testing should occur based on the entire force (i.e., employees and systems at all levels) at ground zero of a predetermined disaster scenario.

For instance, the occurrence of a crisis may incapacitate the operation of the organization in cases where employees are required to attend to family members within a large-scale disaster event, thereby leaving IT systems without the proper necessary attention. Additionally, based on both need and priority, while need spot testing should happen, P6 posits that throwing the main switch (i.e., turning off all IT related applications for personnel and machines) for all levels of functionality is the best way to test an IT DR plan. As such, testing should be a strategic rather than a detrimental factor for an organization during the test. While 100% of participants agree that testing the IT DR plan is critical, they also agree that clients, as well as workers operating in the organization are the first line of defense because once the employee is taken out of the equation, the plan fails instantly. This point is further echoed by participant two who asserts that, “mission first, people always.” When failure is not an option concerning production in a manufacturing MNC or otherwise, one must understand how to test specific networks by location and the disasters that are most likely to transpire (e.g., natural disaster, adversary threat, or terror attack).

Theme 3: Network Location Requirements (Where)

Participant 5 reports**, “**location, location, location, not all IT DR plans are created equal!” According to the Zachman (1987) model, managers use the EIS platform to review locations of strategic technology systems that manage inputs and outputs of a manufacturing organization. Leaders control by location some of the following data and outputs: risk route framework, information systems (IS), logistic information systems (LIS), enterprise resource planning (ERP) for networks, technology sustainment, and opportunities of information systems. P5, who at one point managed over 4,000 IT end-users located in the World Trade Center during the attacks on 9/11 says, “The location of back up data centers is a strategic concern” in all areas of a production organization or otherwise. While 100% of participants mentioned the importance of location for recovery data centers as a strategic concern, Table 2 illustrates the aggregate frequency among the sample of interviews that put the location of data centers as a strategic development over twelve times during participant discussions.

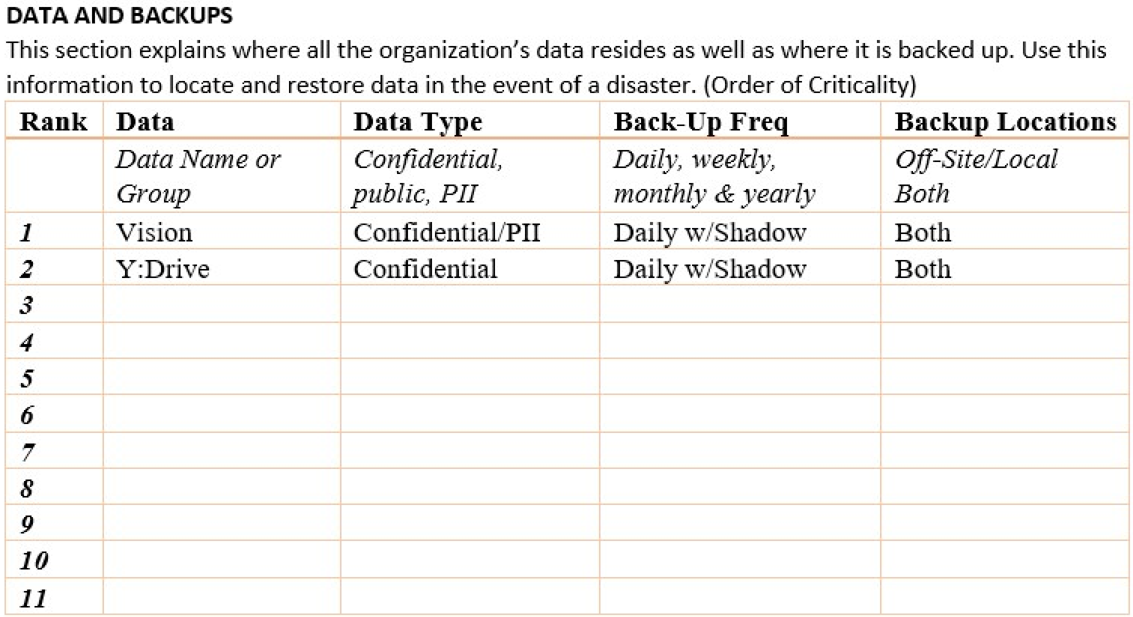
Table 2

Frequency of Strategic Need of Location for Data Centers (Where)

Participant	Interview questions	Total number of references
P1 (M)	1,2,4	11
P2 (D)	2,3,4,5	13
P3 (D)	1,2,3,5	13
P4 (M)	1,3,4,5,6	5
P5 (M)	1,2,6	14
P6 (C)	3	5

Note. Participants with “M” represent employment at a manufacturing organization. Participants with “D” represent a Department of Defense employment that relate to systems in manufacturing. Participants with “C” represent outsource continuity planners that work with several large-scale manufacturing organizations.

For example, if areas of a production factory are destroyed by fire but the data center on location was not, then recovery of data or IT enabled devices are instant in some cases. However, when a production factory is completely destroyed by say an earthquake, then an offsite location data center located in another geographic position, that is not affected by the data loss event, can be used as a recovery asset. According to participants in this study, recovery can be rather quickly, depending on how much data must be recovered and time constraints related to the IT DR plan. Leaders and managers who can create IT DR plans by using off site remote data recovery centers and the availability of using several different locations as remote back-up centers create layers of continuity against IT data loss. As previously mentioned within the study, execution of IT DR through remote technology configurations known as mirror, hot, warm, and cold sites are essential. Figure 5 below illustrates a data backup chart used in IT DR plan, obtained from P1.



DATA AND BACKUPS

This section explains where all the organization's data resides as well as where it is backed up. Use this information to locate and restore data in the event of a disaster. (Order of Criticality)

Rank	Data	Data Type	Back-Up Freq	Backup Locations
	Data Name or Group	*Confidential, public, PII*	*Daily, weekly, monthly & yearly*	*Off-Site/Local Both*
1	Vision	Confidential/PII	Daily w/Shadow	Both
2	Y:Drive	Confidential	Daily w/Shadow	Both
3				
4				
5				
6				
7				
8				
9				
10				
11				

Figure 5. Illustration of written policy concerning Data and Backup charts within an IT DR plan.

Participants agreed that offsite remote recovery data centers where a key strategic development factor in creating IT DR plans within manufacturing organizations or otherwise. According to Lee, Lee, Seong, Rou, and Gim (2019) while all remote technology constructions are based on the size, budget, priority of work, and continuity need, the mirror site technology is the higher cost, essentially allowing mirroring of all data in real-time remotely and requires a large maintenance capability along with the larger budget for construction. P2 stated, “If your main data center goes down you actually have a data center elsewhere that is constantly up and running and replicating data for the main data center; this is known as a hot site.” Lee et al. (2019) further explain that hot sites mirror data, but through replication when an organization experiences a disaster event, data recovery through activation of the remote site with the mirrored capability is a strategic construct. It is notable that IT managers using remote hot site, or mirror technology as a top-level IT DR asset, cannot guarantee 100% data recovery during the transfer of data.

Medium sites are the same configuration of hot sites but come with less cost and only house priority IT requirements; cold sites on the other hand cost the least, but have a longer recovery period (Lee et al., 2019). Lee further posits that cold sites configure space only allocations and data transferred by IT managers occurs only after the disaster occurs. Ultimately, according to written research corroborated by participants within this study, remote back up sites are a strategic requirement for any organization to survive a large natural disaster or manmade event. That said, participants also indicated that “cloud technology” is an added strategic development for data recovery planning.

Another strategic location revealed by participants and used by large, medium, and small manufacturing organizational leaders are virtual storage locations, also known as cloud technology. Virtual storage used for IT DR planning is quickly becoming the norm because this type of configuration simplifies data management, improves operational efficiency, and reduces cost investment (Jun & Lihong, 2017). According to P5 and P6, production organizations use virtual storage technology more regularly, but still require a higher level of security because of its vulnerability to adversary attacks. While IT managers in general agree that cloud technology (i.e., virtual storage) is becoming the norm in IT DR planning, it is more sensitive to manmade attacks and requires an additional back-up requirement. According to participants, remote data centers (e.g., mirror, hot, warm, cold sites) are becoming the second line of defense for the cloud construct if a recovery failure should happen. Participants agreed that offsite data recovery systems work deliberately with cloud storage capabilities as a strategic development means of IT DR planning. That said, all IT DR planning, testing, and recovery configurations have time requirements within a manufacturing organization that directly relate to the type of plan established.

Theme 4: Recovery Time Objectives (When)

Participants agreed that recovery time objectives (RTO) are among the highest strategic developments to IT professionals because recovery time requirements set the stage for IT DR contingency planning. Understanding a manufacturing organization’s RTO allows for implementation of organizational survival during a disaster in four areas: impact analysis, business continuity (BC), incident response (IR), and disaster recovery

(Clark, 2010; Sahebjamnia, Torabi, & Mansouri, 2015). According to participants, the contingency planning management team (CPMT) should first understand the RTO in order to analyze priority IT priority functions that keep the organization resilient during a disaster. Table 3 below illustrates the frequency of time requirements associated with building IT DR plans in manufacturing from participants.

Table 3

Frequency of Strategic Need for Recovery Time Objectives (When)

Participant	Interview questions	Total number of references
P1 (M)	3,5,6	8
P2 (D)	2,6	4
P3 (D)	1,5	4
P4 (M)	1,2,5	5
P5 (M)	2,3,4,6	12
P6 (C)	1,2,5,6	12

Note. Participants with "M" represent employment at a manufacturing organization. Participants with "D" represent a Department of Defense employment that relate to systems in manufacturing. Participants with "C" represent outsource continuity planners that work with several large-scale manufacturing organizations.

Cost and recovery time objectives are different for each priority technology application. P6 explained that it is imperative to, "…know the recovery time objective for the business first when developing an IT DR plan, then test to ensure time constraints can be met." That said, an aggregate of these time allotments might not be able to exceed a certain overall time requirement based on costs in resources, stakeholders, and customer retention. For example, recovery of enterprise IT services that requires software recovery might have an RTO of two hours to find and repair causes to disruptions in hardware, software, IT configurations, and human errors related to a natural disaster or advisory cyber-attack (Franke, Holm, & König, 2014). According to participants five and six, time requirements also define costs associated with different organizations. For example, a large MNC manufacturing company that has overwhelming warehousing capability might have an RTO of days due to the ability to maintain resources needed for production versus a global communications company that might have a couple of hours to regain the entire network. While all participants agreed that understanding the time requirement for recovery is fundamental to priority contingency needs, they also agreed that RTOs help managers and IT professionals to determine cost requirements within the entire business continuity plan.

Lastly, and as detailed in my literature review, leaders use the Business Continuity Plan (BCP) to relate the previous IT DR planning to the level the leaders can relocate an entire organization (Torabi, Giahi, & Sahebjamnia, 2016). In essence, the reaction of IT managers is related to responses that dictate by priority system recovery contingencies and RTO. Leaders and teams use mindful simulated IT recovery contingencies to strategically develop ideas for backup systems, reaction times, and assigned responsibilities to leaders and managers in a disaster.

Theme 5: Cost of IT DR (Why)

Manufacturing organizations in different geographical areas are faced with the threats of natural disasters, terror attacks, or a technological adversary attacks. Therefore, manufactures and their supporting business partners should have a strategic IT DR plan to aid in areas of loss of power and hardware issues, DR testing, security, coordinated off site data center recovery, adequate relocation resourcing, equipment maintenance, backup strategies, and department involvement at all levels of internal and external leadership (Landry & Kroger, 2006; Yang, Yuan, & Huang, 2015). That said, costs associated with the aforementioned areas are part of the IT DR planning process.

Cost analysis is a strategic development for IT DR planning and is varies based on size, type, and capital needs of the organization. Below is a view from other IT DR researchers concerning cost analysis:

> There is not a single blueprint for disaster recovery. Every organization is unique in the applications it runs and the relevance of the applications to its business and the industry therein. Therefore, it is essential to know the main reasons why organizations are willing to pay for such solutions. (Mendonça, Andrade, Endo, & Lima, 2019, p. 519)

According to all participants, there are varied costs associated with manufacturing firms. On one hand, participants agreed that the size of an organization, the RTO, frequency of testing, and higher-level business management buy-in, reflect overall costs of an IT DR plan. On the other hand, the cost associated with not having an IT DR plan far outweighs all other cost requirements because the organization, stakeholders, employees, and product can simply cease to exist after a crisis event. According to participant six, risk management, imagining the highest risk to plan for, testing it, and the amount of priority systems to recovery during the disaster is a critical thought process when calculating costs of an IT DR plan.

According to Rabbani, Soufi, and Torabi (2016), cost benefit analysis for IT DR falls directly on economic factors, recovery time objectives, recovery point objectives, outsourcing partners, and wanted level of continuity by higher management. In all cases, participants agreed that relevance to the size, RTO, priority recovery requirements, and frequency of testing help evaluate the budget requirements needed to develop a strategic IT DR plan. Of these, costs associated with RTO and time allocation for testing are priority strategic developments needed to establish a cost-effective plan. According to participant six, RTO is a priority because there is significant difference in costs associated with two hours to recovery IT networks versus two days, thus, less time equals more cost. Testing the IT DR plan is always a problem in manufacturing because production is time based and activating a complete shutdown to test can create significant costs for real world production requirements.

Applications to Professional Practice

Categorizing effective strategies that IT managers use in IT DR for manufacturing also provides a standard platform for all business organizations to as a resource. Considering the upfront research, participant interview data, and IT standards across all business applications (manufacturing or otherwise) understanding a basis to begin from that assist managers in creating a solid IT DR plan is perhaps the greatest professional application to the industry. As the researcher, I have deduced that business continuity planning, specifically IT DR, is critical for the survival of business in the strategic areas of priority contingency planning, network testing, IT back up locations, time recovery requirements, and costs associated with the IT DR plan. Of these, time, testing, and cost are the most critical strategic applications to professional practice and organizational infrastructure.

One of the main arguments between IT DR planners and other managerial functionalities of professional practice in the manufacturing industry is that time in terms of planning the IT DR and testing the IT DR plays a huge part of the IT DR planning equation. The other argument among professionals is that time costs money, and when a disaster might be very rare, or does not happen at all, what kind of cost is to be allocated to even retain an IT DR plan. There are many opinions on these arguments, but at the end of the day, an organization without a business continuity plan and more importantly, an IT DR plan, could be nonexistent after a major crisis. Applications in time, testing, and cost will help to develop a solid strategic IT DR plan within professional practice.

Time Applications to Professional Practice

Within the study findings, I address time associated to recovery as a strategic area within the IT DR plan and revered as one of the most important. For example, participants indicated the need for an organizational time requirement prior to building the IT DR plan. For example, professional leaders will ask the question, “How much down time are we willing to accept before we are back online with IT applications in communications, supply operations, production, and delivery?” As previously indicated, for some it may be two days, for others it may be two hours, and for some IT leaders it may be a requirement to have zero data loss with no delay whatsoever in production or consumer service. Understanding the time requirements, or the recovery time objective (RTO) sets the stage for levels of contingency, back up locations, priority systems testing, and costs are how leaders apply IT DR within professional practice.

Managers and leaders applying RTO as a professional practice is perhaps the single most important strategic development needed to create IT DR plans. The RTO and recovery point objectives (RPO) mentioned throughout this study are a strategic development requirement. RTO is the maximum time to bring a system or application to its operational state, while the RPO is the maximum amount of lost data in the recovery process (Mendonça, Andrade, Endo, & Lima, 2019). IT managers use RTO and RPO requirements directly to affect DR solutions. Leaders who understand time constraints also understand the effect time has on all other strategic developments, such as level of contingency, back-up locations, type of back-up, priority systems management (e.g. RPO is used by managers allowing them to prioritize network considerations when a disaster first strikes), and costs affecting the entire plan. While time expectations within an IT DR plan are critical, the ability to test a completed plan to ensure managers and leaders meet time requirements is also as essential. Therefore, testing IT DR is a critical application to professional practice in not only manufacturing organizations, but also on other organizations globally.

Testing Applications to Professional Practice

Testing the IT DR plan is another critical strategy application for professional practice. While there are costs associated with contingency testing, the cost associated with not testing after a real-world disaster event is devastating to an organization's survival. While 100% all participants agreed that testing the plan is critical, frequency of testing depends on the size of the organization and level of risk by geographic location. Understanding how and when to test contingency plans in professional practice and updating the plan to close gaps that would otherwise cause the IT DR plan to fail, remains a critical area to incapsulate within a professional application.

When development of the IT DR plan is complete, testing and updating of the plan is an absolute strategic requirement. Zukowski (2014) suggests that only a complete exercise of the plan will lead to refining response and recovery results. He further reinforces the need for testing the DR plan as strategic events that provide information, skills, and capabilities needed when a disaster strikes and is a key application to professional practice. While the need to evaluate and update the IT DR is critical, there is a cost associated with the frequency of testing that includes production loss during testing, stakeholder, employee costs while participating, and costs because of machinery downtime. That said, the costs associated with a manufacturing company staff not developing a strategic IT DR plan is a critical mistake, allowing unneeded risk to potentially wipe out an organization costing the business its existence overall.

Cost Applications to Professional Practice

Lastly, cost analysis of IT DR would be a critical application to professional practice. All participants in this study cited cost as both a negative and a positive factor when developing an IT DR plan. Higher-level managers and leaders automatically react negatively to the costs associated with IT DR, especially if disaster events have not affected the organization over years of operation, if at all. As an IT professional, one must collaborate with management at all functions of the organization in order to not only have an understanding of costs associated with IT DR in place, but also analyze the costs of not having IT DR in place through risk development. In essence, one must weigh the positive and negative risks associated with the IT DR plan concerning cost.

Positive Cost Application to Professional Practice

From a positive cost outlook, participants agreed that IT DR costs help IT managers to strategically pinpoint areas of IT recovery that are critical for the business enterprise. Correctly anticipating costs of IT recovery because of a disaster event in areas of data redundancy, employee preparation, analyzing proper supply chain operations, assessing effects of customers, restoration operations, and testing the plan are positive application to professional practice with acceptable positive costs (Curley, 2014). As previously mentioned within the study, participants agreed that while the IT DR plan can become costly in time, money, and resources, the cost of not having an IT DR plan could be devastating, losing the organization in its entirety and any branding potential of the organization for a potential restart of the enterprise.

Negative Cost Application to Professional Practice

Regardless of the size of a manufacturing organization, or any business enterprise, the bottom line is always the priority when it comes to operational costs. Production managers receive constant pressure from leadership within in an organization concerning costs associated with IT DR planning services because of economic fluctuations in a particular market (Dolewski, 2011). According to all participants in this study, time and money is a primary reason higher levels of management will either shortcut IT DR planning to save other valued resources, or worse, not require an IT DR plan at all. The lesson is clear throughout my research, the cost of not developing a strategic IT DR plan far outweigh the cost of developing one. Selling the need for an IT DR plan to leaders within an organization is a critical application to professional practice. It is also worth noting that many participants in this study agree that cost reflects in the loss of employees, physical property, and degradation of the branding because of consumer temperament during an interruption in service. Selling the need for an IT DR plan to leaders within an organization is a critical application to professional practice and reflects through the employee, stakeholder, and consumer branding of the product.

Implications for Social Change

Strategic IT DR developments for manufacturers, their strategic partners, stakeholders, and consumers facilitate analytical discussions by managers and leaders who are responsible for the resiliency of an organization against natural disasters, terror attack, or adversarial threat. As depicted early on in this research, the implications for social change include IT DR plans that may help prevent economic disruption for consumers, communities, and society during crisis events (Cook, 2015). Inferences of strategic development for IT DR planning, as illustrated in my findings, may increase regional economic resiliency by having affective IT DR plans for business organizations that support local economies by networks online during a crisis while succinctly not affecting supply and demand for customers globally. Additionally, while execution of successful IT DR plans keeps organizations from catastrophic failure, using the basis of strategic IT DR plans as a standard platform requirement in all types of business organizations and worldwide infrastructure is a key implication.

Lastly, understanding strategic IT DR planning requirements can create a standard for all business operations regardless of size or location. For example, using findings in this study, managers and leaders will be able to create a standard for resiliency of large energy corporations during a disaster event. Business leaders and managers will be in a position to apply strategic standards found in my research to implement successful IT DR plans and reduce financial discourse between business operations, stakeholders, consumers, as well as the public in general.

Recommendations for Action

Effective disaster recovery strategies for use by IT managers in the manufacturing industry are critical for business success. According to Carter, Phillips, and Millington (2012) required resiliency of IT applications and networks from internal and external risks associated with a specific organization must be in place to recover successfully during a crisis event. Recommendations for action and the professionals affected seem to logically flow in areas of risk management, contingency planning, time objectives by priority, cost requirements, testing, plan updates, and collaboration with experts in the field within all functionalities of IT DR planning.

Logical Flow of Recommendations for Professionals

Based on my findings, manufacturing leaders and managers should consider the following recommendations as a logical flow when developing strategic IT DR plans. First, IT professionals must determine recovery time objectives by priority networks systems and costs associated with downtime. Secondly, IT professionals along with senior representation of all business functionalities (i.e. staff, operations, logistics, and human resources) should analyze all risks according to natural disasters, terror attacks, or adversary threats by geographic location. Thirdly, managers and leaders should build contingency plans that close gaps found during the risk analysis thereby creating the IT DR plan. Fourthly, IT professionals need to prepare cost requirements associated with both the IT DR plan and costs incurred without a plan and vet this plan through all functionalities of business operations. Finally, business professionals should create frequency of testing requirements and ensure managers and leaders at all levels of the organization understand the resources needed to complete testing and these same IT professionals should update the IT DR plan immediately after testing. Furthermore, IT professionals should be vigilant on innovations and standards through calibration of subject matter experts in the industry. While the recommendations provide a sequential strategic listing for development of IT DR plans, dissemination of recommendations within this study is very important as well.

Dissemination of Findings

IT leaders and managers should disseminate findings within this study as a collaborative effort to IT social events, applicable academic journals, and industry periodicals that will facilitate strategic platform requirements associated with IT DR for all public and private organizations. According to Saracho (2013), propagation of research discoveries through other types of sources is an indispensable component of research progression on any subject. Once my study findings are published, IT professionals can incorporate this research into organizational publications, training circulars, and IT DR initiatives by standard. My intent to personally disseminate these findings include networking with professional business managers not only in U.S manufacturing, but with public and private ventures in infrastructure across the United States, international and global business forums and standards, and to lecture small, medium, and large MNC's within the scope of this application.

Recommendations for Further Research

Managers and Leaders will use findings within this study to contribute further to the development of platform knowledge related to strategic IT DR plans in manufacturing. Further studies in IT DR planning performed by researchers may review the need for established behaviors and experiences required by IT professionals who develop IT DR plans with subjects such as Artificial Intelligence (AI) capabilities of IT networks, contingency planning priorities, review of organizations that manage critical large infrastructure such as national power grids that support business operations, and the need for legislative standard in IT DR requirements. Additionally, based on data collected within the Central United States, further research from a national and perhaps an international perspective may further refine strategic needs for all business organizations and create platform standards for IT DR globally.

Listed within my prospectus concerning this research, limitations are weaknesses within a study that may constrain the output of the project findings (Madsen, 2013). As previously stated, there may be standard processes one uses to develop strategic IT recovery; manufacturing leaders may have different needs depending on types of products, size, sample diversity, and technical requirements needed. As I began to develop themes for this study, it was clear that the standard process includes amaryllis if time, testing, and cost of an ID DR plan, and while different organizations have different needs these three elements are consistent for a successful plan and reducing this limitation. Lastly, a second limitation suggested early in my study that I used only one central framework as a lens for exploring my study topic. Using the Zachman (1987) framework as the only conceptual model may conflict with other related frameworks that will present different outcomes. That said, I openly defined the basis of my research and compare other conceptual frameworks that researchers have used to develop IT recovery strategies such within enterprise information systems.

Reflections

Using a qualitative multiple case study, my research focused on expanding upon finding strategies for the development of IT disaster recovery plans in the manufacturing industry. Reflecting on my involvements through the study methods, I found that regardless of the size of an organization, IT DR experienced strategic planners are a very small group. Furthermore, through this process I had to change from a single case study to a multiple case study in order to find the number of experienced participants that would support data saturation in this area. I found that IT DR is a diverse application among all types of industry and should have universal effects on business communities.

I selected IT DR as my subject of study because it was in this functionality that I needed to expand within my own business acumen. The awareness I gained within the IT DR planning process will not only help me in my business breadth of knowledge but will expand on my further involvement within business continuity applications, higher learning academics, and my pursuit of possibly securing a career with the Department of Homeland Security.

Conclusion

The goal of this qualitative multiple case study was to explore effective strategies that some IT managers in the manufacturing industry use to develop IT disaster recovery plans to support business operations. The cases selected for this study were three manufacturing organizations, one IT continuity agencies, and one department of defense technology center located in the Central United States. Utilizing open-ended questions, I collected and triangulated data to answer the overarching research question. Five themes emerged during data analysis illustrating effective strategies IT managers in manufacturing use to develop IT DR plans. The themes involved (a) contingency planning by priority within a given IT network, (b) testing plans for natural disaster, advisory attack, and human error, (c) network locations and levels of response by crisis, (d) understanding of time requirements for recovery by organization, and (e) costs associated with having a strategic IT DR plan. My findings indicate a need to apply standard strategic solutions for IT DR for business operations. Furthermore, the need for higher level management to agree with testing and development of an IT DR plan financially in order to save the entire organization during a disaster event. Lastly, technology leaders ensure that representation of all business functions and stakeholders have a seat at the table when development of IT DR begins. This will allow for a more synchronized resilient plan at all levels of the manufacturing industry or otherwise.

References

Acar, M. F., Zaim, S., Isik, M., & Calisir, F. (2017). Relationships among ERP, supply chain orientation and operational performance: An analysis of structural equation modeling. *Benchmarking: An International Journal, 24*, 1291-1308. doi:10.1108/BIJ-11-2015-0116

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Qualidade em Pesquisa Qualitativa Organizacional: tipos de triangulação como alternativa metodológica. *Administração: Ensino e Pesquisa, 19*, 66–98. Retrieved from https://raep.emnuvens.com.br/raep/article/view/578

Agus, A., Hassan, Z., & Ahmad, S. (2017). The significant impact of customer relations practices, information technology, and information sharing between supply chain partners on product sales. *Grading Journal for the Social Sciences, 12*, 65-85. Retrieved from http://learningdistance.org

Almeida, R., Linares Pinto, P., Lourinho, R., & da Silva, M. M. (2017). Using visual models for adopting it governance practices. *COBIT Focus, 1*(1), 1-7. Retrieved from http://www.isaca.org

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (CSFS) for information technology governance (ITG). *International Journal of Information Management, 36*, 907-916. doi:10.1016/j.ijinfomgt.2016.05.017

Anderson, S. F., Kelley, K., & Maxwell, S. E. (2017). Sample-size planning for more accurate statistical power: A method adjusting sample effect sizes for publication bias and uncertainty. *Psychological Science, 28*, 1547-1562. doi:10.1177/0956797617723724

Ang, C. K., Embi, M. A., & Yunus, M. M. (2016). Enhancing the quality of the findings of a longitudinal case study: Reviewing trustworthiness via ATLAS.ti. *The Qualitative Report, 21*(10), 1855-1867. Retrieved from https://search.proquest.com/docview/1847465576

Azadegan, A., & Jayaram, J. (2018). Resiliency in supply chain systems: A triadic framework using family resilience model. In Y. Khojasteh (Ed.), *Supply chain risk management* (pp. 269-288). doi:10.1007/978-981-10-4106-8_16

Baham, C., Hirschheim, R., Calderon, A. A., & Kisekka, V. (2017). An agile methodology for the disaster recovery of information systems under catastrophic scenarios. *Journal of Management Information Systems, 34*, 633-663. doi:10.1080/07421222.2017.1372996

Balza-Franco, V., Paternina-Arboleda, C. D., Cantillo, V., Macea, L. F., & Ramírez-Ríos, D. G. (2017). A collaborative supply chain model for non-for-profit networks based on cooperative game theory. *International Journal of Logistics Systems and Management, 26*, 475-496. doi:10.1504/IJLSM.2017.082614

Bala, H., Venkatesh, V., Venkatraman, S., & Bates, J. (2016). If the worst happens: five strategies for developing and leveraging information technology-enabled disaster response in healthcare. *IEEE Journal of Biomedical and Health Informatics*, *20*, 1545-1551. doi:10.1109/JBHI.2015.2477371

Banerjee, P. K., & Biswas, S. (2017). *US Patent No. 9,582,379*. Washington, DC: US Patent and Trademark Office.

Becker, J. (2013). *Examining relationships between hospital inpatient expectations and satisfaction for maximum Medicare reimbursement* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3601243)

Bernard, H. R. (2017). *Research methods in anthropology: Qualitative and quantitative approaches*. New York, NY: Rowman & Littlefield.

Benner, C., & Pastor, M. (2015). Collaboration, conflict, and community building at the regional scale: Implications for advocacy planning. *Journal of Planning Education and Research*, *35*, 307-322. Retrieved from: http://journals.sagepub.com/doi/abs/10.1177/0739456x15580024.

Black, J. T., & Kohser, R. A. (2017). *DeGarmo's materials and processes in manufacturing*. New York, NY: John Wiley & Sons.

Bookbinder, J. H., & Dilts, D. (2016). *Logistics information systems in a just-in-time environment* (SSRN Scholarly Paper No. ID 2801731). Rochester, NY: Social Science Research Network.

Bowen, G. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*, 27-40. doi:10.3316/QRJ0902027

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*, 77-101. doi:10.1191/1478088706qp063oa

Bristowe, K., Horsley, H. K., Shepherd, K., Brown, H., Carey, I., Matthews, B., Murtagh, F. E. (2014). Thinking ahead – the need for early advance care planning for people on hemodialysis: A qualitative interview study. *Palliative Medicine, 1*-8. doi:10.1177/0269216314560209

Brown, T. (2016). *Engineering economics and economic design for process engineers*. Boca Raton, FL: CRC Press.

California Judicial Branch, (n.d). *Disaster recovery framework: A recommendations & reference guide for the California judicial branch*. Retrieved from http://www.courts.ca.gov/documents/itac-dr-framework.pdf

CISSP CIB, (2012). *Common body of knowledge: Business continuity & disaster recovery planning domain*. Retrieved from http://opensecuritytraining.info/CISSP-9-BCDRP_files/9-BCP+DRP.pdf

Carden, L. L., Boyd, R. O., & Valenti, A. (2015). Risk management and corporate governance: Safety and health work model. *Southern Journal of Business & Ethics*, *7*, 137-148. Retrieved from https:// www.salsb.org

Carter, D. L., Phillips, B., & Millington, P. (2012). The impact of information technology internal controls on firm performance. *Journal of Organizational and End User Computing, 24,* 39-49. doi:10.4018/joeuc.2012040103

Cassidy, A. (2016). *A practical guide to information systems strategic planning* (2nd ed.) [DX Reader version]. Retrieved from https://books.google.com/books

Castleberry, Ashley, Pharm D., M.A.Ed. (2014). NVivo 10 software program]. version 10. QSR international; 2012. *American Journal of Pharmaceutical Education*, 78(1), 1-2. Retrieved from https://search.proquest.com/docview/1518528850

Cervone, H. F. (2017). Disaster recovery planning and business continuity for informaticians. *Digital Library Perspectives*, *33*, 78-81. doi:10.1108/DLP-02-2017-0007

Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, *57*, 24-41. doi:10.1016/j.future.2015.09.031

Clark, P. (2010). *Contingency planning and strategies*. In M. Whitman, & H. Mattford (Eds.), 2010 Information Security Curriculum Development Conference (pp. 131-140). doi:10.1145/1940941.1940969

Colorafi, K. J., & Evans, B. (2016). Qualitative descriptive methods in health science research. *Herd-Health Environments Research & Design Journal, 9*, 16-25. doi:10.1177/1937586715614171

Cook, J. (2015). A six-stage business continuity and disaster recovery planning cycle. *SAM Advanced Management Journal, 80*, 23-68. Retrieved from http://samnational.org/publications-2/sam-advanced-management-journal

Curley, H. (2014). Are you prepared? *Business NH Magazine, 31*, 51. Retrieved from https:// www.preparemybtisiness.org

Cooper, M., & Dryden, W. (Eds.). (2016). *The handbook of pluralistic counselling and psychotherapy*. Thousand Oaks, CA: Sage.

Dahlia, D., Togar M., S., & Priyantono, R. (2018). Lessons learned for novice researcher from a qualitative study of a case on continuous ambulatory peritoneal dialysis. *International Journal of Medical Research and Health Sciences, 7,* 106-111 Retrieved from https://doaj.org/article/7fa50073fe0d4682b7346724286feafb

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research*, *3*, 60-95. doi:10.1287/isre.3.1.60

Dolewski, R. (2011). Don’t Bail on disaster recovery planning. *System INEWS, 375*, 27–28. Retrieved from SystemNetwork.com

Dunne, J., & Malone, D. (2016). *Are you being served: A framework to manage Cloud outage repair times for small medium enterprises*. Paper presented at the 2016 27th Irish Signals and Systems Conference (ISSC), Londonderry, England: IEEE. doi:10.1109/ISSC.2016.7528441

Dwivedi, Y. K., Wastell, D., Laumer, S., Henriksen, H. Z., Myers, M. D., Bunker, D., ... & Srivastava, S. C. (2015). Research on information systems failures and successes: Status update and future directions. *Information Systems Frontiers*, *17*(1), 143-157. Retrieved from: https://link.springer.com/article/10.1007/s10796-014-9500-y.

Ebrahimi, A., & Walsh, L. (2018). Improving management education outcomes: Why managers need to understand information technology in today's world. *Ubiquitous Learning: An International Journal, 11*(1), 1-11. doi:10.18848/1835-9795/CGP/v11i01/1-11

Edwards, B., & Cooper, J. (1995). Testing the disaster recovery plan. *Information Management & Computer Security*, *3*, 21–27. doi:10.1108/09685229510088241

Eisner, E. W. (2017). *The enlightened eye: Qualitative inquiry and the enhancement of educational practice.* New York, NY: Teachers College Press.

Erdelj, M., Natalizio, E., Chowdhury, K. R., & Akyildiz, I. F. (2017). Help from the sky: Leveraging UAVs for disaster management. *IEEE Pervasive Computing*, 24-32. doi:10.1109/MPRV.2017.11

Eriksson, B., Durairajan, R., & Barford, P. (2013). *RiskRoute: A framework for mitigating network outage threats*. In K. Almeroth, & L. Mathy (Eds.), Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies (pp. 405-416). doi:10.1145/2535372.2535385

Ferrari, M. (2016). Three disaster recovery mistakes and how to avoid them. *Health Management Technology*, *1*, 20. Retrieved from http://www.healthmgttech.com/

Fiske, S. T., & Hauser, R. M. (2014). Protecting human research participants in the age of big data. *Proceedings of the National Academy of Sciences, 111*, 13675-13676. doi:10.1073/pnas.1414626111

Fleet, D., Burton, A., Reeves, A., & DasGupta, M. P. (2016). A case for taking the dual role of counsellor-researcher in qualitative research. *Qualitative Research in Psychology, 13*, 328-346. doi:10.1080/14780887.2016.1205694

Franke, U., Holm, H., & König, J. (2014). The distribution of time to recovery of enterprise IT services. *IEEE Transactions on Reliability, 63*, 858–867. doi:10.1109/TR.2014.2336051

Galvan, J. L., & Galvan, M. C. (2017). *Writing literature reviews: A guide for students of the social and behavioral sciences*. New York, NY: Routledge.

Garrison, G., Wakefield, R. L., & Kim, S. (2015). The effects of IT capabilities and delivery model on cloud computing success and firm performance for cloud supported processes and operations. *International Journal of Information Management*, *35*, 377-393. doi:10.1016/j.ijinfomgt.2015.03.001

Gerassi, L., Edmond, T., & Nichols, A. (2017). Design strategies from sexual exploitation and sex work studies among women and girls: Methodological considerations in a hidden and vulnerable population. *Action Research (London), 15*, 161-176. doi:10.1177/1476750316630387

Giorgi, E. A. (2017). A response to the attempted critique of the scientific phenomenological method. *Journal of Phenomenological Psychology, 48*, 83-144. doi:10.1163/15691624-12341319

Glaser, B. (2017). *Discovery of grounded theory: Strategies for qualitative research*. New York, NY: Routledge.

Given, L. M. (Ed.) (2008). *The SAGE encyclopedia of qualitative research methods*. Thousand Oaks, CA: Sage. doi:10.4135/9781412963909

Guest, G., Namey, E., & McKenna, K. (2017). How many focus groups are enough? Building an evidence base for nonprobability sample sizes. *Field Methods, 29*, 3-22. doi:10.1177/1525822X16639015

Hatton, T., Grimshaw, E., Vargo, J., & Seville, E. (2016). *Lessons from disaster: Creating a business continuity plan that really works*. *Journal of Business Continuity & Emergency Planning, 10*, 84-92. Retrieved from http://www.businesscontinuityjournal.com/

Hayes, S., Wolf, C., Labbé, S., Peterson, E., & Murray, S. (2017). Primary health care providers' roles and responsibilities: A qualitative exploration of 'who does what' in the treatment and management of persons affected by obesity. *Journal of Communication in Healthcare, 10*, 47-54. doi:10.1080/17538068.2016.1270874

Hendricks, K. B., Jacobs, B., & Singhal, V. R. (2017). *Stock market reaction to supply chain disruptions from the 2011 great east japan earthquake* (SSRN Scholarly Paper No. ID 2959681). Rochester, NY: Social Science Research Network.

Henson, A., & Jeffrey, C. (2016). Turning a clinical question into nursing research: The benefits of a pilot study. *Renal Society of Australasia Journal, 12*, 99-105.Retreived from http://www.cambridgepublishing.com.au/publications/the-renal-society-of-australasia-journal.aspx

Hoeber, O., Hoeber, L., Snelgrove, R., & Wood, L. (2017). *Interactively producing purposive samples for qualitative research using exploratory search*. Retrieved from: ceur-ws.org/Vol-1798/paper4.pdf.

Hong, S. G., Siau, K., & Kim, J. W. (2016). The impact of ISP, BPR, and customization on ERP performance in manufacturing SMEs of Korea. *Asia Pacific Journal of Innovation and Entrepreneurship*, *10*, 39-54. doi:10.1108/APJIE-12-2016-008

Hooki, L., Sungtaek L., JongHyuk S., HoGun., & Gwang,Y. (2019). A technical study of remote backup center performance using public virtual private network. *International Journal of Advanced Computer Research*, *9*(40), 1–10. doi:10.19101/ijacr.srs16002

Hopf, Y. M., Bond, C. B., Francis, J. J., Haughney, J., & Helms, P. J. (2014). Linked health data for pharmacovigilance in children: Perceived legal and ethical issues for stakeholders and data guardians. *BMJ Open,* 4(2) doi:http://dx.doi.org/10.1136/bmjopen-2013-003875

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, *145*, 47-61. doi:10.1016/j.ress.2015.08.006

Hwang, S., Starbuck, R., Lee, S., Choi, M., Lee, S., & Park, M. (2016). High level architecture (HLA) compliant distributed simulation platform for disaster preparedness and response in facility management. In T. Huschka, & S. E. Chick (Eds.), *Proceedings of the Winter Simulation Conference* (pp. 3365-3374). Piscataway, NJ: IEEE Press.

ISO/IEC JTC 1 Information technology [Computer software]. (2008). Retrieved from https://www.iso.org/standard/51639.html

Juiz, C., & Toomey, M. (2015). To govern IT, or not to govern IT? *Communications of the Association for Computing Machinery, 58*, 58-64. doi:10.1145/2656385

Jun, Y., & Lihong, Y. (2017). The cloud technology double live data center information system research and design based on disaster recovery platform. *Procedia Engineering*, *174*, 1356–1370. doi:10.1016/j.proeng.2017.01.289

Khalili, S. M., Jolai, F., & Torabi, S. A. (2017). Integrated production–distribution planning in two-echelon systems: a resilience view. *International Journal of Production Research, 55*, 1040-1064. doi:10.1080/00207543.2016.1213446

Kwong, J. P , Kwong, E. J., Posluns, E. C., Fitch, M. I., McAndrew, A., & Vandenbussche, K. A. (2014). The experiences of patients with advanced head and neck cancer with a percutaneous endoscopic gastrostomy tube: A qualitative descriptive study. *Nutrition in Clinical Practice, 29*, 526-533. doi:10.1177 /088453361453269

Landry, B. J. L., & Koger, M. S. (2006). Dispelling 10 common disaster recovery myths: Lessons learned from hurricane Katrina and other disasters. *Journal on Educational Resources in Computing, 6*. doi:10.1145/1248453.1248459

Landwehr, C., Ludewig, J., Meersman, R., Parnas, D. L., Shoval, P., Wand, Y., Weyuker, E. (2017). Software systems engineering programmes a capability approach. *Journal of Systems and Software*, *125*, 354-364. doi:10.1016/j.jss.2016.12.016

Lane, S. P., & Hennes, E. P. (2018). Power struggles: Estimating sample size for multilevel relationships research. *Journal of Social and Personal Relationships, 35*, 7-31. doi:10.1177/0265407517710342

Lapalme, J., Gerber, A., Van der Merwe, A., Zachman, J., Vries, M. D., & Hinkelmann, K. (2016). Exploring the future of enterprise architecture: A Zachman perspective. *Computers in Industry, 79*, 103-113. doi:10.1016/j.compind.2015.06.010

Lauras, M., Truptil, S., Charles, A., Ouzrout, Y., & Lamothe, J. (2017). Interoperability and Supply Chain Management. *Enterprise Interoperability: INTEROP-PGSO Vision*, *1*, 131-150. doi:10.1002/9781119407928.ch7

Lee, J. Y., Swink, M., & Pandejpong, T. (2017). Team diversity and manufacturing process innovation performance: *The moderating role of technology maturity. International Journal of Production Research, 55*, 4912-4930. doi:10.1080/00207543.2016.1272765

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

Levitt, H. M., Motulsky, S. L., Wertz, F. J., Morrow, S. L., & Ponterotto, J. G. (2017). Recommendations for designing and reviewing qualitative research in psychology: Promoting methodological integrity. *Qualitative Psychology, 4*, 2-22. doi:10.1037/qup0000082

Li, H. J., Chang, S. I., & Yen, D. C. (2017). Investigating CSFs for the life cycle of ERP system from the perspective of IT governance. *Computer Standards & Interfaces, 50*, 269-279. doi:10.1016/j.csi.2016.10.013

Li, J., Tao, F., Cheng, Y., & Zhao, L. (2015). Big data in product lifecycle management. *The International Journal of Advanced Manufacturing Technology, 81*, 667-684. Retrieved from: https://link.springer.com/article/10.1007/s00170-015-7151-x. Accessed 20 Jul 2018.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Newbury Park, CA: Sage.

Madsen, A. K. (2013). Virtual acts of balance: Virtual technologies of knowledge management as co-produced by social intentions and technical limitations. *Electronic Journal of E-Government, 11*, 183-197. Retrieved from http://www.ejeg.com/main.html

Madill, A., & Sullivan, P. (2017). Mirrors, portraits, and member checking: Managing difficult moments of knowledge exchange in the social sciences. *Qualitative Psychology*. https://doi.org/10.1037/qup0000089

Marshall, C., & Rossman, G. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage.

Mathaisel, B. F. (2017). Mitigating the threat of IT business disasters. *The Risk Management Journal, 99*, 34-40. Retrieved from http://www.rmahq.org/

Mendonça, J., Andrade, E., Endo, P. T., & Lima, R. (2019). Disaster recovery solutions for IT systems: A systematic mapping study. *Journal of Systems and Software*, *149*, 511–530. doi:10.1016/j.jss.2018.12.023

Merriam, S. B. (2009). *Qualitative case study research qualitative research: A guide to design and implementation* (2nd ed., pp. 39-54). San Francisco, CA: Jossey-Bass.

Min, D., Hwang, T., Jang, J., Cho, Y., & Hong, J. (2015). *An efficient backup-recovery technique to process large data in distributed key-value store*. In: R. L. Wainright, & J. M. Corchado (Eds.), Proceedings of the 30th Annual ACM Symposium on Applied Computing. New York, NY: Association for Computing Machinery. doi:10.1145/2695664.2696015

Mijumbi, R., Serrat, J., Gorricho, J. L., Latré, S., Charalambides, M., & Lopez, D. (2016). Management and orchestration challenges in network functions virtualization. *IEEE Communications Magazine*, *54*, 98-105. doi:10.1109/MCOM.2016.7378433

Mishra, M. K., Saunders, C. H., Rodriguez, H. P., Shortell, S. M., Fisher, E., & Elwyn, G. (2018). How do healthcare professionals working in accountable care organisations understand patient activation and engagement? qualitative interviews across two time points. *BMJ Open*, 8(10) doi:http://dx.doi.org/10.1136/bmjopen-2018-023068

Mohideen, H., & Dorasamy, M. (2018). Disaster recovery process improvement in it organization: knowledge management and gap analysis. *Journal of Theoretical & Applied Information Technology, 96*, 172. Retrieved from http://www.jatit.org/volumes/Vol96No1/16Vol96No1.pdf

Mufti, F. N., Ahmad, S. M., & Khan, K. S. (2018). Interplay between and influence of Facebook on the academic and social environments of undergraduate university students. *PUTAJ-Humanities and Social Sciences, 25,* 39-54. Retrieved from http://putaj.puta.pk/index.php/hss/index

Nishimura, A., Carey, J., Erwin, P. J., Tilburt, J. C., Murad, M. H., & McCormick, J. B. (2013). Improving understanding in the research informed consent process: a systematic review of 54 interventions tested in randomized control trials. *BMC Medical Ethics, 14*. doi:10.1186/1472-6939-14-28

Nolan, S., Hendricks, J., Williamson, M., & Ferguson, S. (2018). Using narrative inquiry to listen to the voices of adolescent mothers in relation to their use of social networking sites (SNS). *Journal of Advanced Nursing, 74*, 743-751. doi:10.1111/jan.13458

Orser, B. J., Elliott, C., & Leck, J. (2011). Feminist attributes and entrepreneurial identity. Gender in Management: *An International Journal, 26*, 561-589. doi:10.1108/17542411111183884

O'Toole, E., Feeney, L., Heard, K. & Naimpally, R. (2018). Data security procedures for researchers. *J-PAL North America*. Retrieved from https://www.povertyactionlab.org/sites/default/files/documents/Data_Security_Procedures_December.pdf

Özdamar, L., & Ertem, M. A. (2015). Models, solutions and enabling technologies in humanitarian logistics. *European Journal of Operational Research*, *244*, 55-65. doi:10.1016/j.ejor.2014.11.030

Pan, Y. (2017). Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems. *International Journal of Interactive Multimedia and Artificial Intelligence, 4*, 45-54. doi:10.9781/ijimai.2017.437

Papadopoulos, T., Gunasekaran, A., Dubey, R., Altay, N., Childe, S. J., & Fosso-Wamba, S. (2017). The role of Big Data in explaining disaster resilience in supply chains for sustainability. *Journal of Cleaner Production, 142*, 1108-1118. doi:10.1016/j.jclepro.2016.03.059

Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification. *Journal of Marketing Thought, 3*, 1-7. doi:10.15577/jmt.2016.03.01.1

Patten, M. L. (2002). *Understanding research methods: An overview of the essentials* (6th ed.). New York, NY: Glendale.

Patten, M. L., & Newhart, M. (2017). *Understanding research methods: An overview of the essentials*. New York, NY: Taylor & Francis.

Paul, S. K., Sarker, R., & Essam, D. (2015). A disruption recovery plan in a three-stage production-inventory system. *Computers & Operations Research*, *57*, 60-72. doi:10.1016/j.cor.2014.12.003

Pearlson, K. E., Saunders, C. S., & Galletta, D. F. (2016). *Managing and using information systems, binder ready version: A strategic approach*. New York, NY: John Wiley & Sons.

Perrin, A. J. (2001). The CodeRead system: Using natural language processing to automate coding of qualitative data. *Social Science Computer Review*, 19(2), 213-220. doi:http://dx.doi.org/10.1177/089443930101900207

Poslad, S., Middleton, S. E., Chaves, F., Tao, R., Necmioglu, O., & Bügel, U. (2015). A semantic IoT early warning system for natural environment crisis management. *IEEE Transactions on Emerging Topics in Computing*, *3*, 246-257. doi:10.1109/TETC.2015.2432742

Pradhananga, R., Mutlu, F., Pokharel, S., Holguín-Veras, J., & Seth, D. (2016). An integrated resource allocation and distribution model for pre-disaster planning. *Computers & Industrial Engineering*, *91*, 229-238. doi:10.1016/j.cie.2015.11.010

Rabbani, M., Soufi, H. R., & Torabi, S. A. (2016). Developing a two-step fuzzy cost–benefit analysis for strategies to continuity management and disaster recovery. *Safety Science, 85*, 9–22. doi:10.1016/j.ssci.2015.12.025

Rachel, P., Laura-Mae, B., Barbara A., G., & Donna L., B. (2018). Patient, physician, and caregiver perspectives on ovarian cancer treatment decision making: lessons from a qualitative pilot study. *Pilot and Feasibility Studies, 4*(1), 1-8. doi:10.1186/s40814-018-0283-7

Resnik, D. B. (2016). Employees as research participants: Ethical and policy issues. *IRB: Ethics & Human Research, 38*, 11-16. Retrieved from https://www.thehastingscenter.org/

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

Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, *242*, 261-273. doi:10.1016/j.ejor.2014.09.055

Saracho, O. N. (2013). Writing research articles for publication in early childhood education. *Early Childhood Education Journal, 41*, 45-54. doi:10.1007/s10643 012-0564-3

Sarstedt, M., Bengart, P., Shaltoni, A. M., & Lehmann, S. (2017). The use of sampling methods in advertising research: A gap between theory and practice. *International Journal of Advertising, 30*, 650-663. doi:10.1080/02650487.2017.1348329

Saunders, M. N. K., & Townsend, K. (2016). Reporting and justifying the number of interview participants in organization and workplace research. *British Journal of Management, 27*, 836-852. doi:10.1111/1467-8551.12182

Sawik, T. (2017). A portfolio approach to supply chain disruption management. *International Journal of Production Research*, *55*, 1970–1991. doi:10.1080/00207543.2016.1249432

Sechelski, A. N., & Onwuegbuzie, A. J. (2019). A call for enhancing saturation at the qualitative data analysis stage via the use of multiple qualitative data analysis approaches. *The Qualitative Report,* 24(4), 795-821. Retrieved from https://search.proquest.com/docview/2231317021

Sembajwe, L. F., & Kunwar, J. K. (2016). Is informed consent necessary for research on stored human samples? *Arsiv Kaynak Tarama Dergisi, 25*, 119-128. Retrieved from https://doaj.org

Sil, A., & Das, N. K. (2017). Informed consent process: Foundation of the researcher--participant bond. *Indian Journal of Dermatology, 62*, 380-386. doi:10.4103/ijd.IJD_272_17

Snell, R. (2015). Organizations must employ innovative solutions to meet next generation problems. *Journal of Health Care Compliance, 17*, 29-60. Retrieved from https://www.healthcarecompliance.us/journal-of-health-care-compliance.html

Stich, V., Jordan, F., Barmier, M., Oflazgil, K., Reschke, J., & Diews, A. (2015). Big data technology for resilient failure management in production systems. *IFIP Advances in Information and Communication Technology*, *1*, 447-454. doi:10.1007/978-3-319-22756-6_55\s

Strauss, L. J. (2015). Data breach study: Criminal attacks now leading cause. *Journal of Health Care Compliance, 17*, 61-63. Retrieved from http://www.aspenpublishers.com

Sun, L., Karwan, M. H., & Kwon, C. (2015). Robust hazmat network design problems considering risk uncertainty. *Transportation Science*, *50*, 1188-1203. doi:10.1287/trsc.2015.0645

Suzanne Franco. (2016). A doctoral seminar in qualitative research methods: Lessons learned. *International Journal of Doctoral Studies, 11*, 323-339. Retrieved from https://doaj.org/article/31056e2532f44e81845a6303665daafb

Tabaklar, T., Halldórsson, Á., Kovács, G., & Spens, K. (2015). Borrowing theories in humanitarian supply chain management. *Journal of Humanitarian Logistics and Supply Chain Management*, *5*, 281-299. doi:10.1108/JHLSCM-07-2015-0029

Tatoglu, E., Bayraktar, E., Golgeci, I., Koh, S. L., Demirbag, M., & Zaim, S. (2016). How do supply chain management and information systems practices influence operational performance? Evidence from emerging country SMEs. *International Journal of Logistics Research and Applications*, *19*, 181-199. doi:10.1080/13675567.2015.1065802

Taylor, S. J., Bogdan, R., & DeVault, M. L. (2016). *Introduction to qualitative research methods: a guidebook and resource*. Hoboken, New Jersey: Wiley

Thompson, S., Grocke, D., & Dileo, C. (2017). The use of group descriptive phenomenology within a mixed methods study to understand the experience of music therapy for women with breast cancer. *Nordic Journal of Music Therapy, 26*, 320-337. doi:10.1080/08098131.2016.1239648

Tian, W., Zhao, Y., Xu, M., Zhong, Y., & Sun, X. (2015). A toolkit for modeling and simulation of real-time virtual machine allocation in a cloud data center. *IEEE Transactions on Automation Science and Engineering*, *12*, 153-161. doi:10.1109/TASE.2013.2266338.

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, *89*, 201-218. doi:10.1016/j.ssci.2016.06.015

Turel, O., Liu, P., & Bart, C. (2017). Board-level information technology governance effects on organizational performance: The roles of strategic alignment and authoritarian governance style. *Information Systems Management, 34*, 117-136. doi:10.1080/10580530.2017.1288523

Turner, S., Cardinal, L., & Burton, R. (2015). Research design for mixed methods: A triangulation-based framework and roadmap. *Organizational Research Methods, 20*, 243-267. doi:10.1177/1094428115610808

Uddin, M., Hapugoda, S., & Hindu, R. C. (2015). Disaster recovery framework for commercial banks in Sri Lanka. *Journal of ICT Research & Applications*, *9*, 263–287. doi:10.5614/itbj.ict.res.appl.2015.9.3.4

U.S. Department of Health & Human Services. (1979, April). Ethical principles and guidelines for the protection of human subjects of research. Human Subjects Research (45 CFR 46). *The Belmont Report*. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Vandermause, R., Barg, F. K., Perfetti, A. R., Esmail, L., Edmundson, L., & Girard, S. (2017). Qualitative methods in patient-centered outcomes research. *Qualitative Health Research, 27*, 434-442. doi:10.1177/1049732316668298

Vanpoucke, E., Vereecke, A., & Muylle, S. (2017). Leveraging the impact of supply chain integration through information technology. *International Journal of Operations & Production Management, 37*, 510-530. doi:10.1108/IJOPM-07-2015-0441

Vass, C., Rigby, D., & Payne, K. (2017). The role of qualitative research methods in discrete choice experiments. *Medical Decision Making, 37*, 298-313. doi:10.1177/0272989X16683934

Walker, J. L. (2012). Research column. The Use of Saturation in Qualitative Research. *Canadian Journal of Cardiovascular Nursing*, *22*, 37-41 Retrieved from http://www.cccn.ca

Walton, I. (2016). Ethical research. *Midwifery Matters, 1*, 18-20. Retrieved from https://www.midwiferymatters.org/

Walliman, N. (2017). *Research methods: The basics* (2nd ed.). New York, NY: Routledge.

Walsh R.T.G. (2014) Researcher-Participant Relationship. *In: Teo T. (eds) Encyclopedia of Critical Psychology.* Springer, New York, NY

Wang, S., Ouyang, J., Li, D., & Liu, C. (2017). An Integrated Industrial Ethernet Solution for the Implementation of Smart Factory. *IEEE Access*, *5*, 25455-25462. doi:10.1109/ACCESS.2017.2770180

Wilson, E., Kenny, A., & Dickson-Swift, V. (2018). Ethical challenges in community-based participatory research: A scoping review. *Qualitative Health Research, 28*, 189-199. doi:10.1177/1049732317690721

Xu, Z., Sugumaran, V., & Zhang, H. (2015). *Crowdsourcing based spatial mining of urban emergency events using social media*. Paper presented at the 1st ACM SIGSPATIAL International Workshop on the Use of GIS in Emergency Management. New York, NY: Association for Computing Machinery. doi:10.1145/2835596.2835610

Yang, C. L., Yuan, B. J., & Huang, C. Y. (2015). Key determinant derivations for information technology disaster recovery site selection by the multi-criterion decision making method. *Sustainability*, *7*, 6149-6188. doi:10.3390/su7056149

Yin, R. K. (2017). *Case study research and applications: Design and methods* (6th ed.). Thousand Oaks, CA: Sage.

Zachman, J. A. (1987). A framework for information systems architecture. *IBM Systems Journal*, *26*, 276-292. doi:10.1147/sj.263.0276

Zou, Y., Kiviniemi, A., & Jones, S. W. (2017). A review of risk management through BIM and BIM-related technologies. *Safety Science*, *97*, 88-98. doi:10.1016/j.ssci.2015.12.027

Zukowski, R. S. (2014). The impact of adaptive capacity on disaster response and recovery: Evidence supporting core community capabilities. *Prehospital and Disaster Medicine, 29,* 380-7. doi:10.1017/S1049023X14000624

Appendix A: Interview Protocol and Questions

Interview Protocol

A. Introduce self to participant.

B. Verified receipt and/or responds to consent form, answer for any questions and/or concerns of participant.

C. Produce confirmation and acknowledgement that interview is being recorded.

D. Activate recording device.

E. Thank participant for accepting to participate in the study.

F. Start interview with question #1; follow through to final question.

G. End interview and discuss member checking with participant.

H. Thank the participant for partaking in the study. Confirm the participant has contact information for follow up questions and concerns.

I. End protocol.

Interview Questions

Interview Questions

1. How did you assess the effectiveness of these strategies for developing IT disaster recovery plans?

2. What key obstacles did you encounter to the implementation of strategies to develop IT disaster recovery plans?

3. How did you overcome these obstacles to the implementation of strategies to develop IT disaster recovery plans?

4. How have your organization’s IT disaster recovery plans impacted business operations?

5. What additional comments or information regarding strategies to develop IT disaster recovery plans would you like to provide that you have not already shared?

Appendix B: IT Disaster Response Checklist

Disaster Response (DR) Checklist

□ Communications between departments concerning network and critical systems

□ Inventory and complete costs of critical systems (hardware)

□ Performance categories of critical systems (must have or temporary downtime)

□ Risk impacts, and time parameters related to critical systems

□ Network diagram configuration (replication possibilities)

□ Key points of contact for DR event

□ Backup data and power supply

□ Offsite networks and transportation

□ Voice and Email communications related to DR planning

□ Employ network connectivity strategies and tools

□ Testing techniques, outcomes, and adjustments to DR plan