Spring 5-18-2018

A Model for the role of Information Technology leaders in Disaster recovery planning and organizational resilience

Varun Vuppala
La Salle University, vuppalav1@student.lasalle.edu

Rasoola Tyler
La Salle University, tylerr1@student.lasalle.edu

A Model for the role of Information Technology leaders in Disaster recovery planning and organizational resilience

by

Varun Vuppala

and

Rasoola Tyler

A thesis submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Information Technology Leadership

La Salle University 2018

ABSTRACT

Natural and man-made disasters in the past several years have resulted in millions in damages and losses. Despite this, disaster recovery is often not considered by boards as a priority.

This paper will detail the current research on organizational resilience in relation to disaster recovery. It will cover the best practices for IT leaders to prepare for disasters and make their organizations more resilient. It will also show how IT leaders can work to convince their boards to invest in disaster recovery planning and how they can build organizational resilience culture in their organizations through a structured organizational culture change process.

Keywords: disaster recovery planning, leadership, organizational resilience

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF GRAPHS

CHAPTER 1: INTRODUCTION

Statement and Significance of the Problem

A 2002 study by Cerullo and Cerullo found that up to 43 percent of companies impacted by severe disasters never reopened, and a further 30 percent of them failed within 2 years. Yet many organizations have continued to ignore the importance of disaster management and continuity planning. (Sahebjamnia, Torabi, & Mansouri, 2015, p. 262)

As businesses consider how to plan for disasters, there are currently several approaches to disaster recovery planning. The research in this paper analyzes the approaches of previous research on disaster recovery planning and organizational resilience and considers the role of IT leaders in effecting change.

The central topic discussed in this paper is

How IT leaders can affect disaster recovery planning and organizational resilience.

Definitions of key terms

This paper considers information technology leaders to be Chief Information Officer (CIO) or Chief Technology Officer (CTO). While these roles are distinct, they are both referred to throughout the broader literature as IT leaders. Unless specifically referring to something unique to one role, this paper generally will refer to both positions as IT leaders. Medcof (2008) takes a similar tack, “The CTO is usually the highest-ranking technology manager in the firm and in some organizations the position is called Vice President of Technology or some other variant. We will subsume all of these under the most common title, CTO, for ease of discussion.” (p. 406)

Merriam-Webster defines a disaster as a calamitous event bringing great damage, loss, or destruction (Merriam-Webster, 2017). Disaster can be categorized into two areas; natural and man-made. Natural disasters are forces of nature that are unforeseen and may occur without notice (Whitman & Mattord, 2005, p. 56). Some examples of natural disasters are fire, flood, earthquake, lightning, landslides or mudslides, tornado or severe windstorms, hurricanes or typhoon, tsunami, electrostatic discharge, and dust contamination. Man-made disasters usually involve human carelessness or interaction (Whitman & Mattord, 2005, pp. 56-57). Some examples of man-made disasters are chemical fires, oil spills, electrical blackout/brownouts, terrorism or war, and theft.

Disaster recovery is the process of restoring a company to operations.

Whitman and Mattord describe a disaster recovery plan or DRP, as a document intended to provide guidance to the organization in the face of a disaster (Whitman & Mattord, 2005, p. 143). Wallace and Webber treat DRP like any other business project (Wallace & Webber, 2012, p. 2)

Organizational resilience is a combination of disaster recovery and business continuity. It has a focus on people and process while disaster recovery has a focus on technology. Organizational culture is a key component of organizational resilience.

Organizational culture is an important facet of organizational resilience. Ionescu writes, "Organizational culture is an important variable for organizational changes. Through their abilities, managers and leaders have to inspire their employees with a feeling of affiliation to the cultural model of the firm and to remunerate those that through behavior sustain the implementation of change." (Ionescu, 2014, p. 68)

The top management team (TMT), includes IT leaders like CIO and CTO, as well as CEO, CFO and other members of the executive team, also referred to as the board of directors.

Methodology

Significant research has been done on the role of IT leaders and their interaction with management, often referred to in literature as top management team or “TMT”. Literature about organizational resilience fell into two camps – one vein of literature covered frameworks and instruments to measure resilience; the other vein covered resilience in the context of disaster recovery planning.

The structure of the paper is to define what organizational resilience is in relation to disaster recovery planning and to define IT leaders and cover the best practices for IT leaders to prepare their organizations for disasters. The purpose of this paper is to explore models for IT leaders in preparing their organizations for disaster recovery through creating a culture of organization resilience. This model could be measured in future studies. To measure the success of the model, there would need to be a set of variables for each component. The approach of this paper does not include collecting primary data to support the propositions as hypotheses, rather to describe a model and support it through the consideration of published literature and related secondary data.

CHAPTER 2: LITERATURE REVIEW

Disaster recovery, business continuity and organizational resilience

Disaster recovery planning is a challenging and diverse field. For some, disaster recovery, business continuity and organizational resilience are different topics altogether. For others, it is a distinction of degrees. This paper considers disaster recovery to be a key component of organizational resilience.

One perspective is epitomized by Crocetti (2016) who wrote, “DR may be dying. The term DR, that is, not the actual process of disaster recovery. There is a move in the industry to replace the phrase with IT resilience”. Crocetti citing Stephanie Balaouras, vice president at Forrester, states that the main difference between the two terms was time. Balaouras argues that in disaster recovery, downtime was measured in hours to days, while in resiliency, downtime was measured in minutes to hours. Crocetti notes that to John Morency, vice president at Gartner, “resiliency was the new disaster recovery”, and “most Gartner clients don’t use the term ‘disaster recovery’ anymore, they want to focus more on IT resiliency”. (Crocetti, 2016)

Another perspective comes from the research done by Sahebjamnia, Torabi and Mansouri (2014). In their paper, “Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience”, business continuity planning and disaster recovery planning were both considered facets of organizational resilience. They created a mathematical model to help IT leaders determine whether to implement a business continuity plan or a disaster recovery plan when faced with a disaster situation. Their mathematical model, *MOMILP*, would show whether implementing a business continuity plan or a disaster recovery plan would be a better use of resources when an organization faced a disruptive event and needed to be resilient.

Kolay (2017) categorizes organizational resilience in two categories: first-order and second-order adaptive capacity. In this paradigm, first order adaptive capacity is displayed when

organizations bounce back from disasters using pre-existing disaster plans. In contrast, second-order adaptive capacity is when organizations develop new capabilities to respond to situations outside of their immediate control. (p. 301).

Yang, Yuan and Huang (2013) note that 15-20 years ago, “a disaster recovery plan might consist of taking apart a mainframe and drying out the circuit boards in the parking lot with a hair dryer”. (p.6152) Clearly, disaster recovery is an evolving term.

No matter which perspective one subscribes to, the need for IT leaders to have a process to prepare their organizations for disasters is unquestionable. Disasters are getting more frequent and more expensive, all while internal and external customers are becoming more demanding of IT and expecting less downtime. In the coming years, IT leaders will need to take steps to make their organizations more resilient.

The role of IT leaders in their organization will guide how they implement changes. If an organization is structured in a way that IT leaders have little to no power or influence, it would be very difficult to implement changes to make the organization more resilient. Even in organizations with CIOs or CTOs, where IT leaders are represented on the top management team, IT leaders would need to defend the need to spend money on IT disaster planning activities. IT leaders need to be aware of the politics of the TMT and present disaster recovery planning in terms of business benefits.

Sawalha, Anchor and Meaton (2015) describes Continuity Culture as the organizational culture of resilient organizations. Granito (2011) notes that organizational resilience culture is a key component of organizational continuity and argues that organizational culture should be a domain of any IT service management framework. IT leaders can help create a continuity culture through organizational culture change.

Organizational resilience as a concept originated in resilience theory. Resilience as an academic theory started in child psychology, in trying to understand the needs of foster children. (Mallak & Yildiz, 2016, p. 242). It has spread to the Information Technology field as Sahebjamnia, Torabi and Mansouri noted, “the concept of organizational resilience is attracting growing attention among academicians and practitioners”. (Sahebjamnia, Torabi, & Mansouri, 2015, p. 261) This paper considers organizational resilience to have two components – technological and cultural.

High reliability organizations (HRO) were once limited to large banks, hospitals, defense contractors and government agencies. (Weick & Sutcliffe, 2001) John Morency, a vice president at Gartner, noted that the spread of, “newer technologies, such as replication, continuous data protection and snapshotting, are helping organizations enhance resiliency and proactively avoid recovery situations. While recovery time objectives used to be six to 18 hours for many, they’ve dropped to four hours or below” (Crocetti, 2016) This spread of information technology has radically expanded the number of internal and external customers who may expect the mean time to restoration to be almost immediate. It is likely that the differences between business continuity and disaster recovery will continue to shrink as technology and risk analysis improves.

As it relates to organizational culture, organization resilience is the idea that organizations, like individuals, can be resilient and can be taught to be resilient through structured organizational change. (Granito, 2011) A great deal of research has been done on the traits that make organizations succeed despite disasters. One key cultural trait that consistently emerged from the literature review was resilient organizations are willing to change their recovery plans when faced with unexpected inputs. Kolay (2016) notes that an organization’s ability to adapt is at the heart of organizational resilience. (p. 301)

CHAPTER 3: DISASTERS

A key driver for IT leaders to work on disaster recovery planning and resilience is disasters are getting more expensive and more frequent.

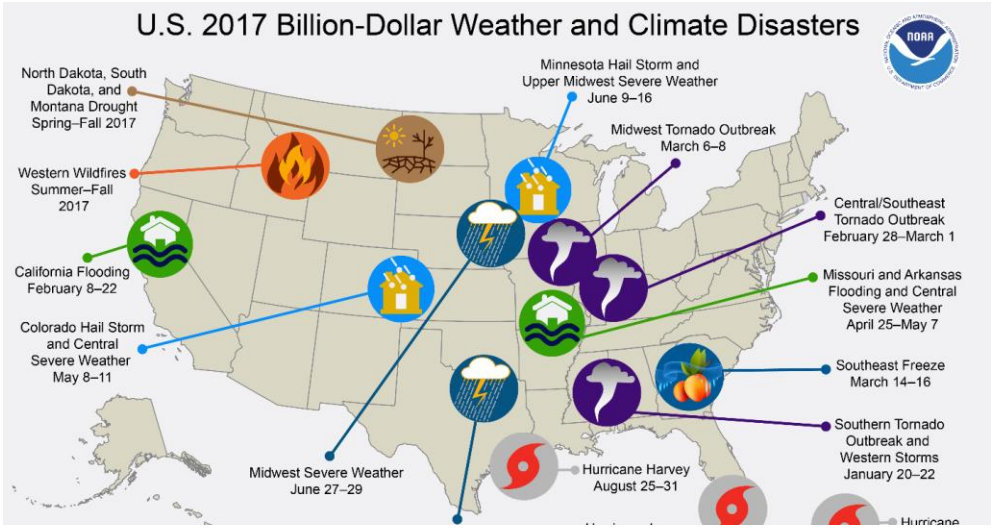
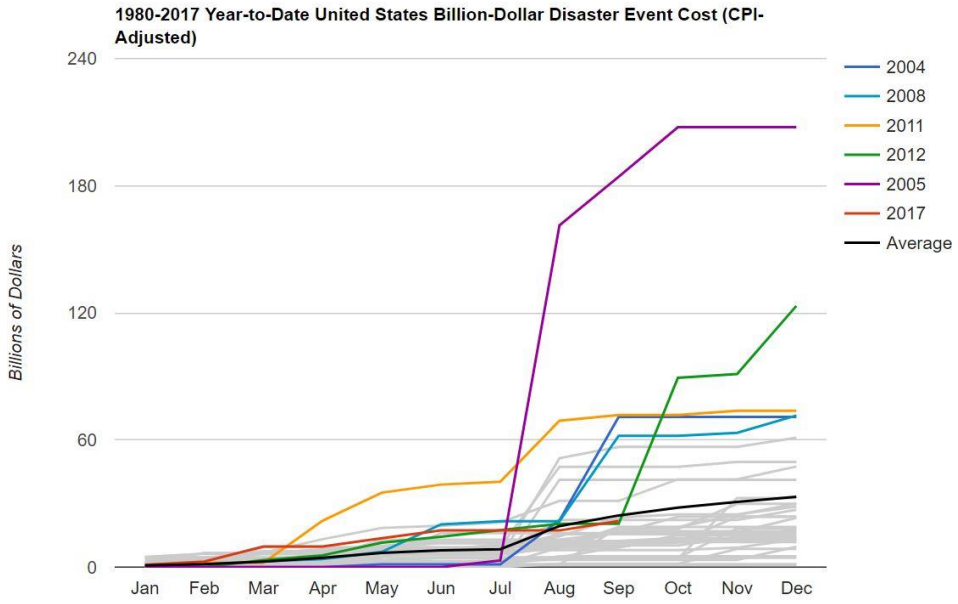


Figure 1 Map of Disaster and Cost in 2017 as of October 6 (NOAA National Centers for Environmental Information (NCEI), 2017)

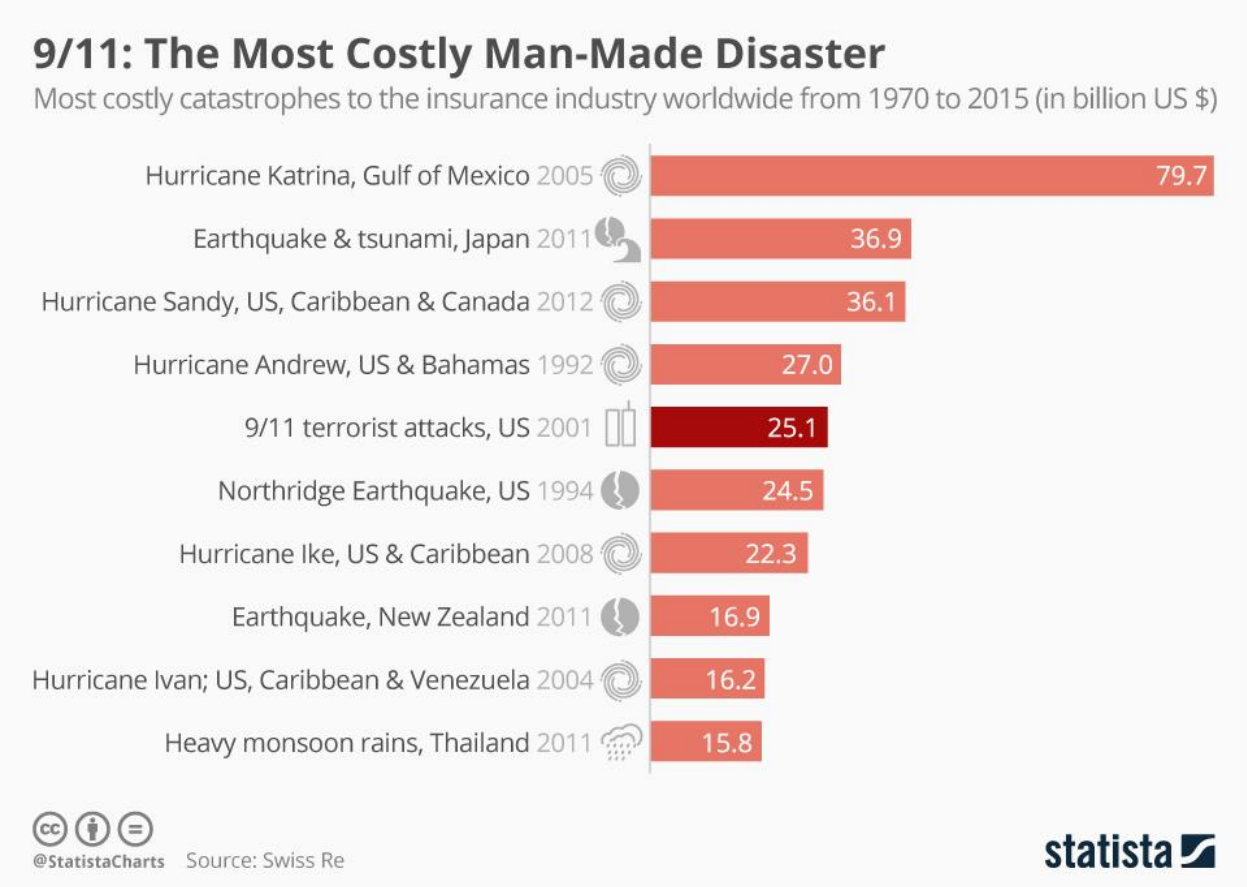
Natural and man-made disasters have become increasingly expensive. Figure 1 is a map from the National Oceanic and Atmospheric Administration (NOAA) National Center for Environmental Information describing all the natural disasters that occurred between January 1st and October 6th, 2017 (NOAA National Centers for Environmental Information (NCEI), 2017). NOAA reported there had been 15 weather events in the United States in 2017 that each caused over a billion dollars of damage.



Graph 1 Graph of Natural Disasters and costs from 2004-2017 (NOAA National Centers for Environmental Information (NCEI), 2017)

Graph 1 plots the cost of natural disasters from 2004 to through the first months 2017; it does not take in account late 2017 storms Hurricanes Harvey, Irma, and Maria. The 2005 disaster costs were between 180 billion dollars and 240 billion dollars. This is due to Hurricane Katrina, which struck New Orleans and two months later Hurricane Wilma which struck the parts of Florida and the east coast (Shabad, 2017).

In 2016, 327 disasters occurred and 127 of the disasters were man-made (Insurance Information Institute, 2017). Man-made disasters include fires, brownouts, terrorism and war. Those disasters resulted in $8 billion dollars in damage. To this date the most expensive man-made disaster was 9/11 terrorist attacks in 2001, which between damage to the World Trade Center and the Pentagon, came to more than $25 billion in damage (Loesche, 2016).



Graph 2 Most Costly catastrophes to the insurance industry worldwide from 1970-2015 (Loesche, 2016)

Graph 2 is a bar graph of some of the disasters and their estimated costs from 1970-2015 (Loesche, 2016). Loesche explains that even though natural disasters are higher, this may be due to poor disaster readiness, for example Hurricane Katrina (Loesche, 2016).

Data center downtime can be quite expensive by the minute. In a 2013 study of U.S. data centers by Ponemon Institute, sponsored by Emerson Network Power, it was found that an unintentional data center outage cost slightly more than $7900 a minute (Sverdlik, 2013). The study also found that the average data center outage of 86 minutes cost about $690,000 and for a partial data center outage of 56 minutes having the average costs of $350,000 in 2013 (Sverdlik, 2013). Planning to recover data centers from a disaster has become a requirement (Omar, Alijani, & Mason, 2011, p. 128).

The role of IT leaders in preparing for disasters

Herbane (2010) covered the changing role of IT leaders in disaster recovery planning, noting that the first era, was "functional rather than strategic" and was prompted in large part by financial companies preserving data for auditing in the wake of the 1977 Foreign Corrupt Practices Act and other similar laws. (p. 982) Herbane notes that by the 1990s, there was a transition rapidly occurring from classical disaster recovery which was technical in focus towards business continuity, which was focused on restoring service operations. He notes that, "without the stewardship of senior management, the need and importance of disaster recovery would fail to reach a wider constituency" (p. 983).

Herbane describes the current phase as "acceleration and focus." (p. 978). In this phase, an IT leader can play a critical role in preparing an organization for disasters and in coordinating the response to disasters. IT leaders can provide the stewardship that Herbane noted was lacking in previous eras of disaster recovery. Boin (2014) notes that leaders have, "an often-overlooked task: to nurture resilience before a crisis occurs (p. 138). van der Hoven et al (2012) argued that IT leaders should show leadership, "in being a spokesperson for technology, a strategist, and a director of corporate R&D" (van der Hoven, Probert, Phaal, & Goffin, 2012, p. 25). The fluidity of the roles makes it possible for IT leaders to reorient the roles towards building resilience through integrating best practices.

The challenge IT leaders will face is to convince their boards that organizational resilience is something that should be in the portfolio of the CIO or CTO instead of another leader. Herbane notes that in 1999, Rodetis argued that CPAs should have a core role due to their "experience with risk identification and management." (Herbane, 2010, p. 984)

IT leaders will need to demonstrate awareness of business needs and approach the board politically. A key challenge noted across the literature is convincing management that there is sufficient business case for making changes to the disaster recovery plan, without a clear-cut way to show that a return can be made on any investment in changes.

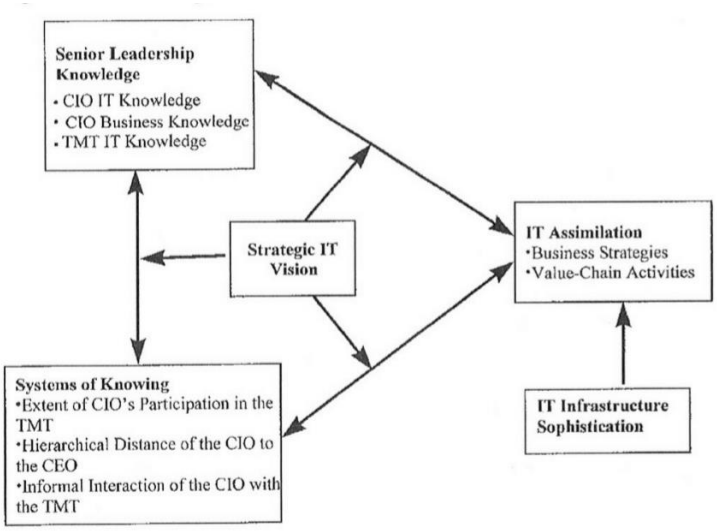


Figure 2 Conceptual Model (Armstrong & Sambamurthy, 1999, p. 306)

Figure 2 from Armstrong and Sambamurthy (1999), shows the components of the CIO's influence. IT leaders should be framing disaster recovery and organizational resilience not as IT expenses, but in terms of the business benefits. Several studies have covered ways to measure the effectiveness of IT efforts. Granito created the OCD, a way to measure the effectiveness of organizational culture change. (Granito, 2011)

IT leaders must develop other bases for influence which are largely informal, such as: strong personal relationships with the CEO and other influential people, a strong informal network both inside and outside the organization, a significant ownership position in the firm, expertise in matters other than technology including an intuitive grasp of business issues and good knowledge of the corporation and its environment. (Medcof, 2008, p. 419)

Monica Brink describes types of pushback that IT leaders may get from their top management teams:

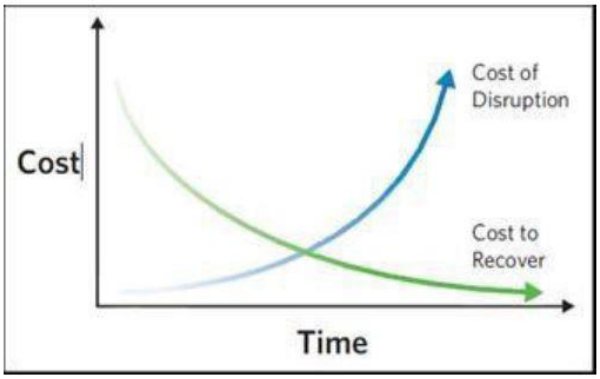
- More IT disaster planning would incur great costs.
- The company already stores backups on site.
- The location does not experience severe weather.
- The company has few downtime events.
- The company never experiences outages. (Brink, 2017)

Adding a disaster recovery to the IT budget does not have an immediate benefit and may be considered a sunk cost. Disaster recovery plans are planning for the uncertain. An organization may think full redundancy of their data centers would be required for a disaster recovery plan, however Brink suggests other methods such as cloud computing Disaster Recovery as a Service (DRAAS) can be obtained to whatever specs an organization may need (Brink, 2017). Having a backup system locally does little if the disaster strikes locally. The backups may be affected and take many hours to restore data. Again, a cloud computing solution can be beneficial because it is offsite and may take only minutes to restore service (Brink, 2017).

Being in a region with relatively pleasant weather is not an excuse to neglect disaster recovery precautions. Brink noted that some disasters may be man-made caused by lack of attention by the organization or its partners (power plant, ISP, gas company, etc.) (Brink, 2017). Since IT leaders are not in control of these incidents, it is necessary for them to create and implement a robust disaster recovery plan to ensure organizational resilience.

Brink states not having stoppages or outages is unrealistic (Brink, 2017), however companies will be forced to adopt shorter recovery times to maintain a competitive advantage as technology makes it possible to further reduce time to recovery. Downtimes and outages can also

tarnish an organization's brand, for example Amazon.com cannot afford to be down at any time, because many companies rely on their services to conduct business. According to Amazon's SLA they guarantee monthly uptimes of 99.99% to their clients or service credits will be rendered (Amazon, 2017).



Graph 3. Cost to Recover vs Cost of Disruption (Prazeres & Lopes, 2013, p. 796)

Graph 3 shows the cost to recover versus the cost of disruption (Prazeres & Lopes, 2013, p. 796). The cost of recovery increases with the shorter time-to-recover requirements, however the cost of disruption increases the longer the unit is down (Prazeres & Lopes, 2013, p. 796). The point where the two curves cross would be the optimal disaster recovery goal.

This focus on disaster recovery planning does not hurt competitiveness. Amazon's offer to credit customers for any downtime is not specific to them, other businesses which compete in the same field, including Box.com and Microsoft have similar offerings in their SLAs. IT leaders need to convince the TMT that investing in IT will make the organization more resilient.

One theme that is clear from the various sources is that IT leaders need to be proactive in communicating with the TMT and be political in forming coalitions to advance their goals. Schobel & Denford (2013) argue that the TMT is not a team, and IT Leaders may get better results by making individual connections with individual TMT members. Their research shows that the CIO role may have a natural ally in the CFO (p. 262). Johnson & Lederer (2005) studied

the effects of communicating frequently with the CEO and found that IT leaders who established a communication channel were more effective in getting results (p. 241); to wit, CIOs who emailed the CEO frequently were more likely to be considered closely by the CEO when making decisions.

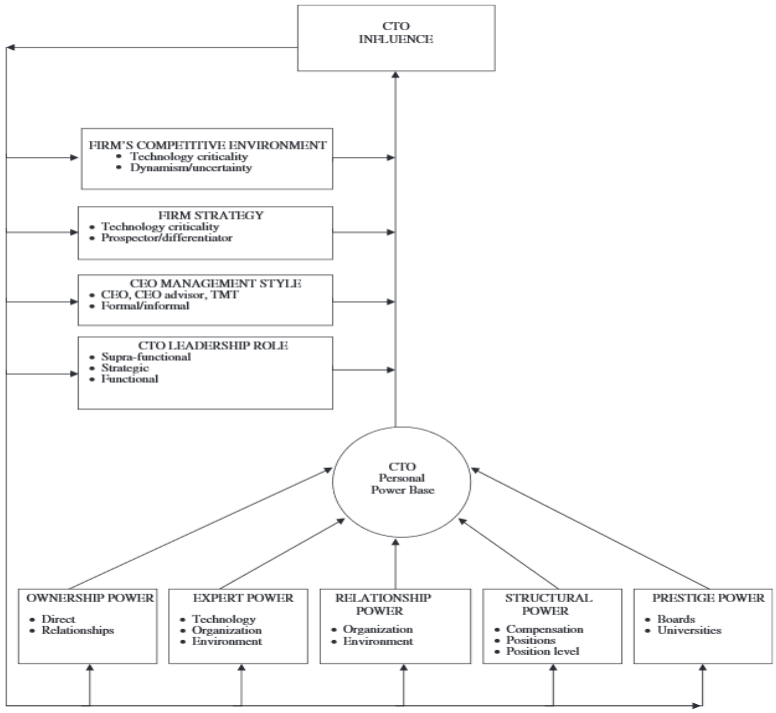


Figure 3 The dynamics of Chief Technology Officer (CTO) power and influence. (Medcof, 2008, p. 415)

Figure 3 shows the dynamics of an IT leader's power and influence, drawing from interpersonal relationships with the board of directors, a network of support inside and outside the organization, and technical expertise in matters other than technology, especially a grasp of business issues and good knowledge of the corporation and its environment (Medcof, 2008). The five parts of an IT leader's power base are:

- Ownership power comes from making good relationships with business sponsors or directly owning the project.
- Expert power comes from technical knowledge of the systems and processes and organization.

- Relationship power comes from creating a large and varied network of allies throughout the organization.
- Structural power comes from having a formal position in the organizational hierarchy, on the board.
- Prestige power results from effective positions with prestigious members of the board.

Overall, successful IT leaders must be politically savvy to gather support on the TMT for their strategic vision. It may involve being intentional about communicating frequently with the CEO, it may involve allying with the CFO. Building a wide power base by nurturing good working relationships with business sponsors and maintaining expertise as a technologist, especially since boards are still not very IT-aware – as Yayla cites Cloyd (2012), "a recent study revealed that half of the 860 public companies surveyed spend less than 5% of board time discussing IT–related risks and opportunities". (Yayla, 2014, p. 405).

CHAPTER 4: DISASTER RECOVERY PLANNING

Classical disaster recovery planning attempts to identify known risks. Kadlec and Shropshire (2010) describes DRP in the cycle illustrated in figure 4 below (p. 3). Each stage is described below.

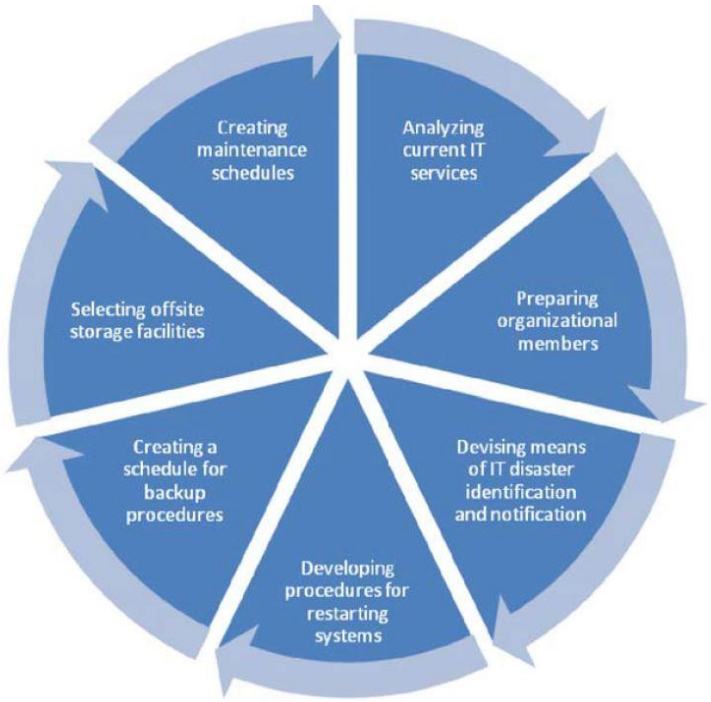


Figure 4 Disaster Recovery Planning Circle (Kadlec & Shropshire, 2010, p. 3)

The first stage is to analyze current IT services. This will consist of listing all services and assessing all risks. Identification of key IT services should include people, procedures, data assets, hardware, software, and network assets (Whitman & Mattord, 2005, p. 227). Identification of people should be noting each employee's position, role, or function, also if they are a supervisor, the security clearance level, and specialized skills. This stage should identify all the procedures, define the purpose of a procedure and relate to software/hardware/networking elements in the organization (Whitman & Mattord, 2005, p. 227). Procedure identification also includes storage locations for reference and update. Data should be classified by owner, creator,

and manager, noting the size of the data structure, type of database sequential or relational, data location in the cloud or locally, and current backup procedures that are practiced (Whitman & Mattord, 2005, p. 227). Hardware, software, and networking assets should be noted. Make, model, serial number, location, and purpose of the hardware should be included in this identification. Software licenses, purpose, operating systems, and install procedures should also be identified. Networking assets should be documented as hardware, and be identified including name, IP address, media access control address, type, and relationship to the network map. Networking assets should also identify the administrator and the department it services in the organization.

Risk is the possibility an event will occur and the severity that event will harm the organization (Wallace & Webber, 2012, p. 37). Whitman and Mattord added that during the analysis phase one must establish main trepidations, the first is ensuring people are safe, and second is preserving the integrity of the data (Whitman & Mattord, 2005, p. 226).

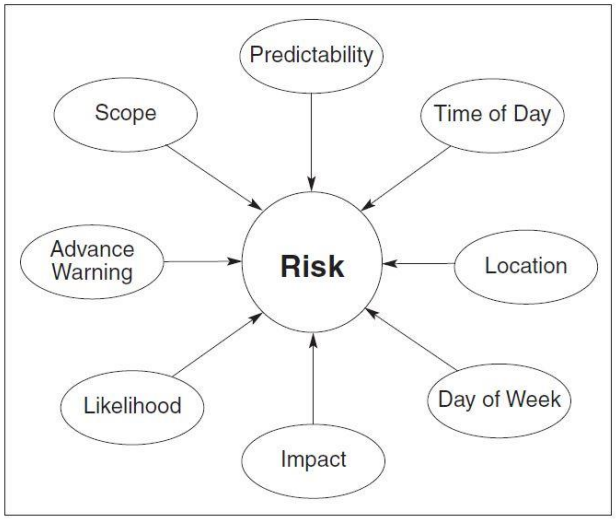


Figure 5 Attributes of Risk (Wallace & Webber, 2012, p. 37)

Figure 5 shows the risk attributes. Wallace and Webber suggest IT leaders should build a risk analysis table based on these attributes. These risks should be weighted, with a touch of mistrust (Wallace & Webber, 2012, p. 37). This risk analysis will be useful in creating a risk

assessment, which compares risks to certain controls that are already in place (Wallace & Webber, 2012, p. 38). Risks are not always known. A good DRP should be able to address unforeseen risks, such as a sudden flood or fire, however DRP does not work well for unknown risks such as a consequence of a flood due to a hurricane. This was the case for Hurricane Katrina in 2005, and Hurricane Maria in 2017. In the case of Hurricane Katrina, the unknown risks, were the faulty flood control system and ill designed levee system (Kim, 2012). In the case of Hurricane Maria, a fragile electrical infrastructure and high winds that destroyed trees, powerlines and homes, leaving many residents without power months later (Erdman, 2017).

The next stage is preparing organizational members. Kadlec and Shropshire suggest there should be a formal teaching of decision making groups consisting of the disaster recovery team preparation and non-team preparation. The decision-making structure should be formalized. (Kadlec & Shropshire, 2010, p. 4). Whitman and Mattord (2005) simplify this stage, stating there should be a clear assignment of accountabilities (p. 226). Everyone on the disaster recovery team should aware of their responsibilities during a disaster. People should be given responsibility for coordinating with local emergency groups, others for clearing employees from the facilities safely, and others accountable to pack up and leave (Whitman & Mattord, 2005, p. 226).

The third stage is devising a means of IT disaster identification and notification (Kadlec & Shropshire, 2010, p. 4). Kadlec and Shropshire label three elements in this stage, detection, warning, means of warning (Kadlec & Shropshire, 2010, p. 4). A person or automated system should identify the disaster. DRP procedures should assign someone to follow an alert roster that consists of first responders, insurance agencies, the disaster recovery team, and key stakeholders including management teams and administrators (Whitman & Mattord, 2005, p. 226). Enterprise

Technology Park in Philadelphia provides 24/7 disaster recovery services to its customers (Philadelphia Technology Park, 2012). If an IT leader were to subscribe their company to Enterprise Technology Park's disaster recovery services, they would be included on the third-party company on the alert roster. The means of warning would be an established means of communication, such as a special phone, instant messaging system or email.

The fourth stage of DRP is developing processes for restarting IT Services and systems (Kadlec & Shropshire, 2010, p. 4). Technical recovery plans are necessary for any good DRP (Wallace & Webber, 2012, p. 85). Ranking of what systems should be restored first should be documented. Wallace and Webber (2012)suggested that services should be returned based on critical business purpose (p. 97).

The fifth stage is creating backup schedules for data, software, configuration files, along with reviewing IT disaster recovery plans (Kadlec & Shropshire, 2010, p. 4). When backing up databases Mullins suggests that you answer the following questions about your database and organization. These questions should aid in database design and database disaster recovery planning

- How much daily action transpires against the data?
- How often does the data get changed?
- How critical is the data to the business?
- Can the data be redesigned effortlessly?
- What kind of access do the users need? Is 24/7 access required?
- What is the penalty of not having the data available during a recovery? What is the dollar value related with each minute of interruption? (Mullins, 2016, p. 50)

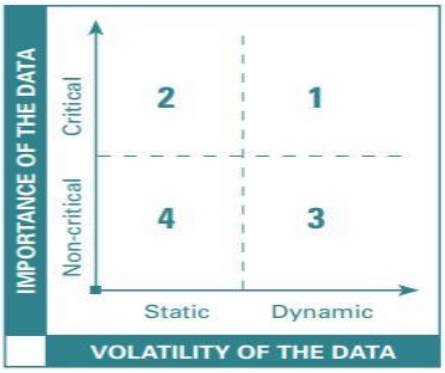


Figure 6 Volatility of Data Chart (Mullins, 2016, p. 50)

In Figure 6, Mullins suggests data be catalogued by its importance and volatility (Mullins, 2016, p. 50). Quadrant 1 describes data that is critical and constantly changing. This data requires routine backup and is vital to an organization's business function. This data should be backed up frequently, and immediately available for recovery. Quadrant 2 is critically static data. This data does not change a lot, but it is critical to business functions. Mullins suggests this data is backed up weekly in incremental backups (Mullins, 2016, p. 50). Quadrant 3 is non-critical but dynamic. This is data that can be easily recreated. It could be a batch job that is recreated nightly or printed data that can be re-entered in the system. Weekly backups of quadrant 3 data would be sufficient. Quadrant 4 data is non-essential and static data. Mullins describes this data as non-essential and should only be backed up after the other three quadrants are backed up (Mullins, 2016, p. 50).

The sixth stage is selecting off-site storage facilities (Kadlec & Shropshire, 2010, p. 4). A successful DRP selects the best offsite facilities that includes the traits of transportability and locality (Kadlec & Shropshire, 2010, p. 4).

The final stage of DRP is creating a maintenance schedule for the organization (Kadlec & Shropshire, 2010, p. 4). A maintenance schedule should account for Information Technology innovations, changes in laws, and changes in organizational structure. Wallace suggests the

Business Continuity Manager tests the plan quarterly. The emergency back-up services should have the capacity to execute critical applications, back-end servers should be correct to handle data and users, and network connections should be protected, both internal and external (Wallace & Webber, 2012, p. 162).

Extending Disaster Recovery Planning into Organizational Resilience

Disaster recovery planning is essentially a mature and well-understood practice at large companies. At the enterprise end of the spectrum, an organization may have disaster recovery plans for each line of business.

In her symposium, "Leadership during Crisis", Robin Kielkowski, the Vice President of Global Business Continuity at BNY Mellon, described having managed, "over 1,300 recovery plans in multiple lines of business". In preparation for Superstorm Sandy, BNY activated a recovery plan. Employees from areas not hit by the storm would come in to assist affected areas. At the last minute, the storm shifted course and hit a different part of the coast. Suddenly, "those who planned to be in a support role suddenly were in recovery mode, and those who planned for the impact changed roles to support the areas hit". (Kielkowski, 2013) The value of organizational resilience here is to be able to adapt to events that were not part of the disaster recovery plans. Organizational resilience is in this context an extension of disaster recovery planning with the added flexibility of adapting to unexpected events.

Disaster Recovery Planning works well when recovering from known risks, however when there is an unknown risk such as in the case of Hurricane Maria or 9/11, the recovery efforts may fail. Wagner and Disparte (2016) suggests organizations need to have a form of risk agility to combat the unknown by learning from events and combining them with instinctual methods to maintain business continuity (Wagner & Disparte, 2016, p. 14). The top-down

approach present in DRP may not prove beneficial during multifactor events (Boin, 2014). If all the information about the event is not known, such as flooding from Hurricane Katrina, it could change the results of a DRP. Boin suggests that organizational leaders also shouldn't fall in to traps.

- *Sticking to the plan and not improvising when needed*. Well thought out plans fail for unknown or inimitable events. Being able to think outside the box leads to a more resilient organization.
- *Waiting for all the information on the disaster to be gathered before acting.* In the beginning of the event the information may not be correct or even worse the time transpired waiting for a complete assessment of the calamity could lower chances to make serious resolutions.
- *Using all resources to regain communication before taking other actions.* Leaders may want to reconnect the internet or phone services to gather information, but that may take a lot of time, which could be used to recover other systems.
- *Assuming the command and control structure will withstand chaos.* In the face of pending danger well thought out DRP's may fail. Leaders need to be flexible and able to deal with highly stressful situations.
- *Waiting for external assistance.* Leaders may want to wait for outside help or offsite restoration, however each minute waiting could be hazardous to critical recovery stages (Boin, 2014).

The seventh stage of the DRP described a maintenance schedule. This stage leads to organizational resilience because reviewing and revising DRPs will allow organizations to

discover innovative methods to recover from a disaster and discontinue outdated efforts. Google tests its business procedures once a year during their system-wide fatigue testing coined Google DiRT (Krishnan, 2012). They continuously strive to find weaknesses in their continuity plans.

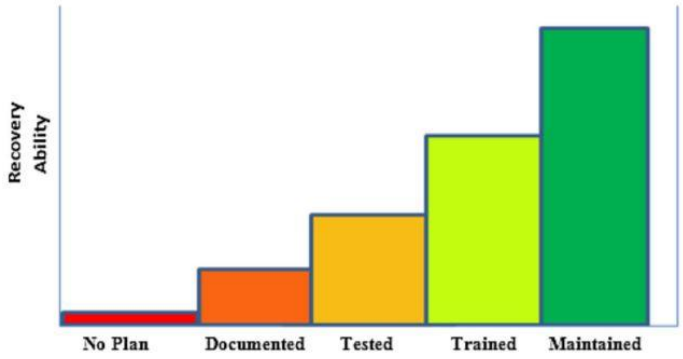


Figure 7 Ability to recover versus BC Plan Maturity (Sawalha, Anchor, & Meaton, 2015, p. 431)

Figure 7 depicts a bar graph described by Sawalha, Anchor, and Meaton, is recoverability vs the development of organizations business continuity plans (Sawalha, Anchor, & Meaton, 2015, p. 431). The higher the level on the scale the more likely the organization can recover from an adverse event.

During a disruptive event, several plans may be available to managers to implement. It is important to have an integrated way to gauge which plans to implement or else managers would have to know, "when and how to switch from continuity phase to recovery phase, while making a trade-off between continuity and recovery plans, and arranging resources [after experiencing] disruptive incidents" (Sahebjamnia, Torabi, & Mansouri, 2015). IT leaders must plan to ensure their teams know when to use a business continuity plan, when to use a disaster recovery plan, and when to abandon preplanned activities and start unplanned resilience activities.

CHAPTER 5: CREATING A RESILIENCY CULTURE

Many of the components of disaster recovery planning are technical – redundant off-site servers, data backups, etc. A non-technical component is organizational culture. van der Hoven et al noted that in 2001, a large-scale study of CTOs found that organizational culture was sixth in a list of their top 24 concerns. (van der Hoven, Probert, Phaal, & Goffin, 2012, p. 26) Ionescu notes that, "Organizational culture is an important variable for organizational changes. Through their abilities, managers and leaders have to inspire their employee with a feeling of affiliation to the cultural model of the firm and also to remunerate those that through behavior sustain the implementation of change." (Ionescu, 2014, p. 68)

The idea of integrating a concept into every stage of the lifecycle is not new. Past organizational culture efforts have included Total Quality and Secure SDLC. For example, Newbold and Azua (2007) describe how the CIO of IBM managed to create a culture change through the introduction of the Technology Adoption Program. By creating and iterating on a collaborative intranet site, they were able to increase employee engagement significantly. The site led to a great deal of collaboration and then innovation and so the project serves as a valuable example of the way IT leaders can influence organizational culture (Newbold & Azua, 2007). Integrating resilience into every project would work similarly. Each stage in the project lifecycle would have a component that encouraged thoughtful consideration of how the project would relate to the organizational goal of resilience. The business impact analysis at the start of a project would consider the business sponsors' requirements in terms of time to restore. The continuous service improvement process would consider how the project could be more resilient after each disaster type event.

Sawalha et al (2015) looked at the role of organizational resilience in Jordan, and described resilient organization culture as, “continuity culture”. (Sawalha, Anchor, & Meaton, 2015, p. 429) Ionescu (2014) writes “Leadership plays a crucial role in creating and maintaining an evolutionary, change-oriented organizational culture” (Ionescu, 2014, p. 66)

Weick and Sutcliffe describe the culture of traditional high reliability organizations as having five parts- deference to expertise, a preoccupation with failure, a reluctance to simplify interpretations, a sensitivity to operations and a commitment to resilience. (Weick & Sutcliffe, 2001, p. 10) Weick and Sutcliffe describe deference to expertise as a culture shift to push more decision making down the chain of command so that front-line employees feel more engaged. A preoccupation with failure as a part of the culture involves encouraging reporting of mistakes and errors and openly discussing even small mistakes to ensure that they are corrected. A reluctance to simplify interruptions in IT may be conducting a full root cause analysis as part of a post implementation review. Sensitivity to operations in terms of IT would be continuous service improvement, a focus on constantly improving things even without failures. Finally, a commitment to resilience is a mindful approach to improving the organization. Weick and Sutcliffe describe this type of resilience as “a combination of keeping errors small and of improvising workarounds that keep the system functioning.” (Weick & Sutcliffe, 2001, p. 14)

Granito (2011) identifies a lack of a domain in change methodology for organizational culture change. Granito notes that organizational culture is a key part of several change models. He argues that structured IT change frameworks like IT Service Management (ITSM) and IT Infrastructure Library (ITIL) should have a domain focused on how organizational culture change is tied to organizational resilience. (Granito, 2011)

CHAPTER 6: ORGANIZATIONAL CHANGE MODELS

An IT leader will need to act as a catalyst to influence change in an organization. There are many different models that describe organizational change. Lewin's model explains change as "Unfreezing", "Movement", and "Refreezing" (Cumming & Worley, 2015, p. 22). Chacko does not provide a model; however he does state disaster operation management (DOM) planning should include those in the community that will be directly impacted by procedures and policies implemented (Chacko, 2014, pp. 13-14). Ionescu describes the change management process like any other decision-making process containing three stages: anticipating, operational and final measurement, and understanding of the results (Ionescu, 2014, p. 69).

IT leaders must use an organizational change model such as the Action Research Model, to change the culture of the organization. The Action Research Model focuses on change as a recurring process (Cumming & Worley, 2015, p. 24). All future actions are determined by initial research. Action Research can help organizations implement detailed planned changes and develop general knowledge that could be applied to other settings. It is assumed that key stakeholders will bode well using this model to develop a DRP/BCP, because it identifies the problem, resolves it, works with feedback from the group, then revises the plan. Several key sections of the model stand out, “problem identification, consultation with a behavioral science expert, data gathering and preliminary diagnosis, feedback to key client or group, joint diagnosis of the problem, joint action planning, action, data gathering after action” (Cumming & Worley, 2015, p. 24). The action research model is an efficient method to begin planning for a disaster, at the joint planning stage, more drilled down planning procedures are desired. Data gathering, and feedback will be achieved with live tests of the DRP/BCP or actual disasters. This model is applied, because on the IT leader level a global organizational change is desired for developing

the best DRP/BCP encompassing all areas of business. Trends have moved the action research model from smaller subsets of the organization to total systems and communities (Cumming & Worley, 2015, p. 25)

The first stage of the Action Research Model is identifying the problem. Cummings and Worley (2015) describe this stage as when the executive, or IT leader, senses an organization has one or more problems that might be solved with an organizational development practitioner (p. 24). In comparison to the Lewin Model, this is part of the "Unfreezing" stage. The IT leader sees a need for change in the current disaster recovery plan. It is possible the organization does not have an adequate plan, or the plan is not updated. The problem identification stage is where the IT leader recognizes there is a problem with the current disaster recovery plan and he/she must devise a way to influence the organization to strive for organizational resilience.

The next stage is for the IT leader to bring in an organizational change expert. The organizational development practitioner may be internal or external, and they may have their own development theory. However, the IT leader should make sure that it meshes with their goals (Cumming & Worley, 2015, p. 24). While launching a campaign to revise or create a disaster recovery plan, the organizational development practitioner should be share his/her methodology with the IT Leader. He/she should collaborate with the IT leader in all aspects of the planning realm.

The third stage of the Action Research Model applied to disaster recovery planning is gathering all data and determining a preliminary assessment of the problem (Cumming & Worley, 2015, p. 24). This step is where the IT leader will engage with department leads to find weaknesses that may be present in respective departments. There are four basic methods of gathering data; questions, process inspection, surveys, and organizational performance data

(Cumming & Worley, 2015, p. 24). They should be able to provide extensive risk assessments of departments identifying what would happen if certain hardware or procedures would be affected if a portion was to go down due to a disaster. IT leaders should ask which redundancies are in place. Beaty (2013) warns that redundancy is a critical issue for data centers, and most data centers should have a tier system be it parallel or series to make the data center more reliable (p. 122). With this knowledge, IT leaders and the organizational development practitioner will be able to use this information to come up with the current health of the organization. This stage places disaster recovery planning and organizational resilience on everyone's mind.

The fourth stage is feedback to the major stakeholders. During this stage findings are shared with the groups. The Organizational Change expert provides all the relevant information to the major stakeholders and their groups (Cumming & Worley, 2015). Collaborations of risk assessments with the consultant and the groups allow everyone to discuss which strengths and weaknesses the organization's related hardware, to policy, and procedures when facing a disaster. This vital stage keeps the planning transparent and involves the stakeholders, which bodes well in creating a successful DRP/BCP.

In the fifth stage, a combined analysis, the IT leader should work with the consultant and the group to share feedback and analyze the problems, in this case creating or revising a proper disaster recovery plan. Cummings and Worley cite Edgar Schein, paraphrasing action research is different from the doctor patient model, where the doctor gives a diagnosis and a solution. (Cumming & Worley, 2015). On the other hand, in this stage of Action Research everyone agrees on what the problem is, in the case of DRP/BCP, and need of revision. IT leaders should

allow their group to recognize the problem to ensure that a sense of ownership is gained, so that subsequent cultural changes would be more readily accepted.

The beginning of the moving process as described in Lewin's model is stage six, which is named joint action planning (Cumming & Worley, 2015, p. 25). The consultant and the organization jointly devise a disaster recovery plan and business continuity plan. Subsequent iterations of all these steps lead to organizational resilience, because the ability to take what was learned in the past to anticipate the future need is incorporated. Everyone will work to change the culture, technology, and environment by creating a plan that takes in to account the best policies and procedures for disaster recovery and business continuity plan.

The action stage is the seventh stage. The disaster plan is shared with the organization. All facets of the organization should be well trained and ready to face any disaster that may befall the organization. A thorough disaster recovery plan will lead to organizational resilience, because the organization will be prepared to improvise during the unexpected storm or man-made disaster.

The final stage is data gathering after the action. This is the feedback stage for the disaster recovery plan. A stress test which may be taken during an actual or planned disaster, for example Google DIRT (Krishnan, 2012, p. 48). Information is gathered during the disaster and the IT leader and the organization will assess the plan and return to stage 4 (feedback to key client or group). This is a cyclical process that creates a more tempered disaster recovery plan over time. IT leaders should revisit these steps annually to keep the DRP/BCP from growing stale.

CHAPTER 7: CONCLUSION

IT leaders need to take steps to prepare their organizations for disasters, including disaster recovery planning and creating a resilient organizational culture. The models described in this paper would allow IT leaders to make an impact on their organization and prepare the organization for responding to disasters effectively – creating disaster recovery plans, working politically to engage other members of the TMT and convince business sponsors that there is solid business value in IT working on organization resilience, and implementing culture change throughout the organization through structured culture change management.

Gaps in current research

The primarily limitation with this thesis is generalizability. This thesis was focused on IT leaders at organizations that have CIO or CTO roles and may not be generalizable to other organizations where IT is not represented effectively on the TMT. Another weakness is that these frameworks and studies all represent an organization's ability to react to an event, which means that there is no one-size-fits all solution for each organization to follow. This paper also does not cover theft, or data breaches of the types that many retail companies recently experienced.

The strength of this paper was performing an exhaustive literature review on organizational resilience and disaster recovery. In analyzing the literature, we have identified several gaps in the existing research. Current research does not address the role of IT Leaders in creating organizational resilience culture in organizations.

There are few peer-reviewed articles that address the role of IT leaders in both disaster recovery planning and organizational resilience. This analysis utilized existing publicly available literature. Most companies do not publicly share their disaster recovery plans. This limits the

ability to draw broad conclusions about the extent to which disaster recovery planning has matured and the extent to which the push for organizational resilience has changed processes and beliefs.

Future research

Future research into the subject area could include creating a survey instrument and soliciting responses from CTOs and CIOs in large and mid-size companies on their attitudes towards disaster recovery and organizational resilience. A survey instrument would provide data on the arguments set forth in this capstone– that disaster recovery planning and organizational resilience both need to be implemented to prepare organizations for disasters.

Surveys of Fortune 100 companies would help to understand how they developed their disaster recovery plans and surveys of CIOs/CTOs to assess their level of autonomy in acting in disaster situations would provide information for future work on extending the role of IT leaders.

REFERENCES

Amazon. (2017, November 15). *Amazon EC2 Service Level Agreement*. Retrieved from AWS: https://aws.amazon.com/ec2/sla/

Armstrong, C. P., & Sambamurthy, V. (1999). Information Technology Assimilation in Firms: The Influence of Senior Leadership and IT Infrastructures. *Information Systems Research*, 304-327.

Beaty, D. (2013). Managing redundancy. *ASHRAE Journal, 55(7)*, 122.

Boin, A. (2014). Designing Resilience - Leadership Challenges In Complex Administrative Systems. In e. a. Louise K. Comfort, *Designing Resilience: Preparing for Extreme Events* (pp. 129-142). University of Pittsburgh Press.

Brink, M. (2017, January 4). *Why you can't let disaster recovery slide off your IT budget in 2017*. Retrieved from CloudTech: https://www.cloudcomputing-news.net/news/2017/jan/04/why-you-cant-let-disaster-recovery-slide-your-it-budget-2017/

Chacko, J. (2014, December 8). Sustainability in disaster operations management and planning: An operations management perspective. *ProQuest Dissertations & Theses Global*, pp. 1-208.

Crocetti, P. (2016, June 2). *IT resilience vs. disaster recovery: What's better for your business?* Retrieved from SearchStorage.com: https://searchstorage.techtarget.com/blog/Storage-Soup/IT-resilience-vs-disaster-recovery-Whats-better-for-your-business?vgnextfmt=print

Cumming, T., & Worley, C. (2015). *Organization Development and Change.* Stamford, CT: Cengage Learning.

Erdman, J. (2017, October 20). *Why Hurricane Maria was Such a Castrophy in Puerto Rico*. Retrieved from The Weather Channel Hurricane News: https://weather.com/storms/hurricane/news/2017-10-19-why-hurricane-maria-puerto-rico-catastrophe

Granito, F. A. (2011). Organizational Resilience and Culture a Model for Information Technology Service Management (ITSM). *Dissertation*, 96. Ann Arbor, Michigan, United States of America: ProQuest Dissertations Publishing. doi:ProQuest ID 1019235444

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History, 52(6)*, 978-1002. Retrieved March 15, 2018, from https://www.tandfonline.com/doi/abs/10.1080/00076791.2010.511185

Insurance Information Institute. (2017, November 16). *Facts + Statistics: Man-made disasters*. Retrieved from Insurance Information Institute: https://www.iii.org/fact-statistic/facts-statistics-man-made-disasters

Ionescu, V.-C. (2014). Leadership, Culture and Organizational Change. *Manager Journal, 20*, 65-71. doi:ProQuest ID 1684456227

Johnson, A. M., & Lederer, A. L. (2005). The Effect of Communication Frequency and Channel Richness on the Convergence Between Chief Executive and Chief Information Officers. *Journal of Management Information Systems*, *22*(2), 227-252. doi:10.1080/07421222.2005.11045842

Kadlec, C., & Shropshire, J. (2010). Best practices in IT disaster recovery planning among US banks. *Journal of Internet Banking and Commerce, 15(1)*, 1-11. Retrieved September 19, 2017, from

http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/503236647?accountid=11999

Kielkowski, R. (2013). Leadership During Crisis. *Journal of Leadership Studies, 7*(3), 62-65. doi:10.1002/jls.21300

Kim, S. D. (2012). Characterizing unknown unknowns. *PMI® Global Congress 2012—North America, Vancouver, British Columbia, Canada.* Newtown Square, PA: Project Management Institute.

Kolay, M. K. (2016). Measurement of Organizational Resilience - An Approach. *Productivity, 57*(3), 300-309.

Krishnan, K. (2012). Weathering the unexpected. *Communications of the ACM (55)11*, 48-52.

Loesche, D. (2016, September 9). *The Most Costly Man-Made Disaster*. Retrieved from Statista: https://www.statista.com/chart/5772/costliest-man-made-disaster/

Mallak, L. A., & Yildiz, M. (2016, July 5). Developing a workplace resilience instrument. *Work, 54*(2), 241-253. doi:10.3233/WOR-162297

Medcof, J. W. (2008). The organizational influence of the Chief Technology Officer. *R&D Management, 38*, 406-420.

Merriam-Webster. (2017, 11 08). *"Disaster"*. Retrieved 11 08, 2017, from Merriam-Webster: www.merriamwebster.com/dictionary/disaster

Mullins, C. S. (2016). Determining your database backup schedule. *Database Trends and Applications, 29(6)*, 50. Retrieved November 22, 2017, from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1762651169?accountid=11999

Newbold, D., & Azua, M. (2007). A model for CIO-led innovation. *IBM Systems Journal, 46*(4), 629-637.

NOAA National Centers for Environmental Information (NCEI). (2017, November 17). *U.S. Billion-Dollar Weather and Climate Disasters* . Retrieved from NOAA National Centers for Environmental Information (NCEI): https://www.ncdc.noaa.gov/billions/

Omar, A., Alijani, D., & Mason, R. (2011). INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN: CASE STUDY. *Academy of Strategic Management Journal, 10(2)*, 127-141. Retrieved November 19, 2017, from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/886538620?accountid=11999

Philadelphia Technology Park. (2012, November 12). Enterprise Technology Parks Partners with Recovery Networks to Provide IT Disaster Recovery to Customers Affected by Hurricane Sandy. *Information Technology Newsweekly*, p. 543. Retrieved November 20, 2017, from http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1179000342?accountid=11999

Phipps, C. (2014, August 19). *Organizational resilience: yet another buzz word?* Retrieved from Continuity Central Archive: http://www.continuitycentral.com/feature1217.html

Prazeres, A., & Lopes, E. (2013). Disaster Recovery – A Project Planning Case Study in Portugal. *Procedia Technology, 9*, 795-805. Retrieved November 20, 2017, from https://www.researchgate.net/publication/273822464_Disaster_Recovery_-_A_Project_Planning_Case_Study_in_Portugal

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

Sawalha, I. H., Anchor, J. R., & Meaton, J. (2015). Continuity Culture: A Key Factor for Building Resilience and Sound Recovery Capabilities. *International Journal of Disaster Risk Science*, 428-437.

Sawalha, I., Anchor, J., & Meaton, J. (2015). Continuity culture: A key factor for building resilience and sound recovery capabilities. *International Journal of Disaster Risk Science, 6(4)*, 428-437.

Schobel, K., & Denford, J. S. (2013). The Chief Information Officer and Chief Financial Officer Dyad in the Public Sector: How an Effective Relationship Impacts Individual Effectiveness and Strategic Alignment. *Journal of Information Systems, 27*(1), 261-281. doi:10.2308/isys-50321

Shabad, R. (2017, September 4). *How Hurricane Harvey's cost stacks up against past disasters*. Retrieved from CBS News: https://www.cbsnews.com/news/how-hurricane-harveys-cost-stacks-up-against-past-disasters/

Sverdlik, Y. (2013, December 4). *One minute of data center downtime costs US$7,900 on average*. Retrieved from Data Cener Dynamics: http://www.datacenterdynamics.com/content-tracks/power-cooling/one-minute-of-data-center-downtime-costs-us7900-on-average/83956.fullarticle

van der Hoven, C., Probert, D., Phaal, R., & Goffin, K. (2012). Dynamic Technology Leadership The Adaptive Role of the CTO. *Research-Technology Management*, 24-33.

Wagner, D., & Disparte, D. (2016). *Global Risk Agility and Decision Making - Organizational Resilience in the Era of Man-Made Risk.* London: Palgrave Macmillan.

Wallace, M., & Webber, L. (2012). *The Disaster Recovery Handbook : A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets.* . New York, NY: AMACOM.

Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty.* San Francisco: Jossey-Bass.

Whitman, M. E., & Mattord, H. J. (2005). *Principles of Information Security.* Boston, MASS: Thomson Course Technology.

Yayla, A. A. (2014). The Effect of Board of Directors' IT Awareness on CIO Compensation and Firm Performance. *Decision Sciences, 45*(3), 401-436.