*i*Journals: International Journal of Software & Hardware Research in Engineering (IJSHRE)
ISSN-2347-4890
Volume 9 Issue 2 February 2021

A Brief Analysis on the Existing Disaster Recovery Phases and Activities Plans

Mustapha Atiku[1], Adamu Abdullahi Garba[2] and Aliyu Musa Bade[3]

[1] Information and Media Technology Department Main Campus, Gidan Kwanu, P.M.B 65, Minna, Niger State, Nigeria

[2.3]Department of Computer Science, Yobe State University Damaturu, Nigeria

Mustapha_atiku@gmail.com[1]; adamugaidam@gmail.com[2]; albad0007@gmail.com[3]

ABSTRACT

Disaster recovery planning is a vital necessity of any kind of organization that is a small-large enterprise. Disaster recovery is a part of business continuity and deals with the immediate impact of the event; it might be recovering from a server outage, security breach. Disaster recovery planning is the preparation that is done for any kind of disaster that has occurred whether artificial or natural cause. However, the successful execution of a disaster recovery plan phase is contingent upon the effectiveness of its strategy. Having the right information available at the right time for the current situation is crucial to make the right decision in a timely fashion. Because a Wrong or late decision in an emergency can have a huge impact on the safety of people and the business. This research paper focuses on analyzing the various existing disaster recovery phases and activities plan. The paper would serve as an entry point for new researchers on disaster recovery and also benchmark for improving the recovery phases and activities.

Keywords: Disaster recovery, organization, existing Plan

1. INTRODUCTION

Information security is vital in the general public largely as a consequence of our nearly pervasive embracing of computing technology, in our everyday lives which many of us work with computers for our employers, go to school online buy goods from traders, go-to a coffee shop with our laptops to check there emails and our bank balances. Although this technology makes us be more productive and allow us to access a host of information with only a click of the mouse, it also comes. With a great host of security issues. If the information on the system used by our employers and our bank becomes exposed to an adversary the consequences will be severe. According to Andreason (2009) is defined as "guarding information and information systems from unlawful access, use to expose interruption, modification, or destruction" in a nutshell it means we want to defend all our data (wherever it is) and systems and organizational assets from those who will like to misappropriate them. Whitman et, al (2013) security of a computer system must be designed to protect confidentiality, availability, and integrity of the information system. This shows that Information security is alarmed with the confidentiality, integrity and availability of data irrespective of the arrangement the data may take: electronic, print, or other forms. Information Security refers to the procedures and approaches which are designed and executed to protect print, electronic, or any other method of confidential, private and sensitive information or data from unapproved access, use, misuse, disclosure, destruction, modification, or disruption. This paper aims to analyse the existing disaster recovery phases and activities plans and proposes disaster recovery phase to serve as benchmark for future research.

2. INFORMATION SECURITY MANAGEMENT

Securing data assets inside association that arrangement is running involve a sequence of data protection of organization businesses which is intended for protection. Data protection is comprehensive, and involves a colossal scope of fields, this displays the dependability of assorted department to data protection in organisations. All

association in all fields depends mainly on data resources and reliable data depends on how the association strategically apply protection of information. As top association bureaucrat's locale highlighting on data protection at a crucial level next probable the data protection of such association will be elevated, it is extensively trusted by researchers that the top down way of data protection implementation is extra prosperous than the bottom up. A strategy plays a extremely meaning act in data protection management. Enterprise and association have strategies, standards and guidelines for a reference intentions ant it stays as a driver for the organisation. Data protection 12 standards are necessity and it can be utilized to furnish a larger period for a robust data protection association.

2.1 Contingency Planning:

According to Rouse (2014) contingency plan is a procedure that formulates an organization to react comprehensibly to an unintended event. A contingency plan is sometimes referred to as "Plan B," because it can be also used as a different for action if expected results fail to materialize. Contingency planning comprises component of business continuity, disaster recovery. Contingency planning is developing reactions in advance for various situations that might impact business. Although undesirable events perhaps come to mind first, a good contingency plan should also address positive events that might mess up operations - such as a very large order. Every business has the possibility of a situation that adversely impacts operations. If the response to the situation is poor, it might have a dramatic impact on the future of the business - loss of customers, loss of data, even loss of the business.

2.2 Disaster Recovery Plan

Disaster recovery plan has not received attention in mainstream is research, which boast of only articles that were published in peer reviewed MIS journals in the past ten years. In order to rectify this; IT disaster identification and notification, preparing organizational members, IT services analysis, recovery process, backup procedures, offsite storage and maintenance. These seven dimensions represent the collective actions that firms need to take in order to ensure recovery post it disasters. Disaster recovery plan is critical and developing the plan the first place. According to Rothstein, (2007), many organisation to develop a plan let alone finding the resources and time to conduct meaningful testing. Thus disaster recovery recovers the disrupted IT and telecommunication capabilities to ensure critical business functions can continue within planned level of Disaster Recovery Planning is about defining consistent, pre-planned actions that will react to various Disaster Scenarios. In other words, Disaster Recovery Planning is about reacting to the Disaster Scenario after it has happened space.

3. SOURCE OF DISASTER

According to a survey human error is responsible for 40% of all the data loss and hardware or system failure is 29% (Snedaker 2013). International business machine (IBM) conducted a study to determine data loss due to human error is 80% (Woodie, 2010). Although people are responsible for designing creating implementing as well as observing activities and process to safeguard data integrity. Thus disaster planning is all about recovering after event whereas business continuity is planning for future trends to your organisation and looking for alternative solutions to mitigate or avoid disruptions. The idealism of having a DRP is to aid in avoiding hazards before disruption and how to recover data after disruption.

Process in DR comprises of two component the planning and the implementation phase thus the process organisation follows for their routine business are the key to long term business success for example if a business is hit by a disaster then the process is interrupted immediately. Process are created and used in handling diverse disaster and emergency scenarios, obviously disasters are caused by either artificial or man-made disaster however artificial disasters are usually caused by malicious users whose main aim is to bring down the organisation information system or delete their data. Theft, blackmail, and online attacks such as hacking, virus worm, terrorism and sabotage are some causes of disaster. Ware as natural disasters are caused by nature such as volcanic eruption, flood, land slide, etc. some of the common natural disaster includes physical destruction, fire draught and weather events technical disaster like power failure, communication, network failure, system failure and server failure respectively. The impact of disaster and the risks it posed to the organisation can be easily calculated using the level of impact

analysis disaster can occur at any time, some can be expected due to the level of risks it posed to the organisation a time when threat is identified and priorities it would already be too late figures 1.1 elaborates on the occurrences of disaster in US organizations.

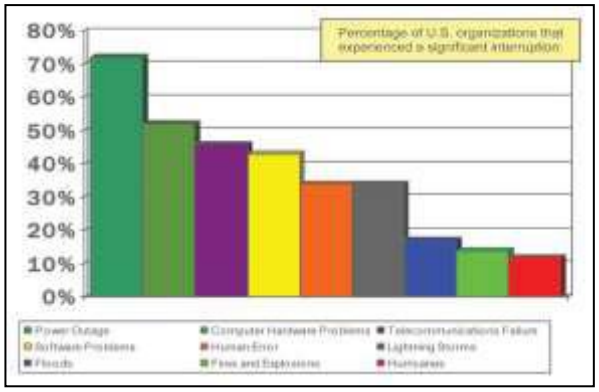

Figure 1.1 Percentage of U.S. organization that experienced a significant

As seen in Figure 1.1, 72 percent of U.S. organizations have experienced significant interruption and loss of returns caused by power outages, with 52 percent experiencing computer hardware problems. The size and scope of these events have caused business executives to rethink their business continuation strategies and consider increases in capital expenditures for disaster recovery services. If any of these events occurred and business was affected, how long would the business be able to remain out of production without suffering detrimental returns loss.

3.1 Man-Made Disaster

The computer follow instruction given by the user of the system, therefore it cannot make mistake on its own. The user of the technology defines the application of it whether for good or bad circumstances. Many researchers have argued that almost 80% of information problem related to computer is because of people working on the technological sector mostly, the man made failure can be further being divided into two categories: intentional and unintentional damage. Unintentional failure can be closely related to the lack of proper discipline in the area of work such as employee in an organization using computer without following the rules and regulations of using computer, which sometimes lead to loss of vital information. The second phase which is intentional is mostly link to the intentional damage or stealing of organizational information for either fun or other benefit. Figure 1.2 shows the types of malware.

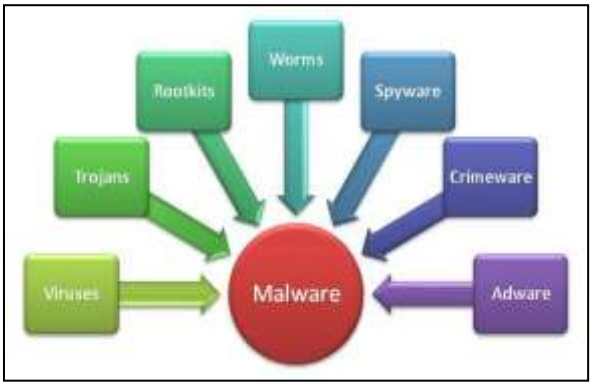

Figure 1.2 Man-made disaster Sources (Stephen, 2014).

3.2 Natural Disaster

Natural disaster such as fire, floods, tornadoes, earthquakes can cause significant damage to the organisation and result in data loss. Thus, any large disaster has the degree to damage your data Solomon (2013). Data is a raw fact and securing data is essential to any organization that depends on IS for its operations. Protecting the confidentiality, integrity and availability of data is a measure goal of every organization globally. Data disaster recovery in an organisation, data can be stored traditionally and as well as sing technology to store, process and retrieve information faster. Though technology comes with its pros and cons. attackers and hackers can easily temper with an organisation information in order to disrupt their business and reputations. The data disaster recovery can be classified into three components; data or information, hardware and software disaster recovery. Since most business are digital now, digital crime is on the increase, digital crimes are committed by exploiting the known vulnerability of software. Thus, one of the common virus attacks to organisation is virus.

4. Types of Disaster Recovery Sites

Backing up the data is one of the first considerations that are invoked in a disaster recovery plan according to Wells et al (2006) when doing disaster recovery testing its advisable to do it with normal back up. There are many ways to backup data, data can be stored to a CD's, DVD's, Disks, tape depending on the data to be backed up and the recovery methods chosen according to the organizations requirement many companies have a record retention policy that dictates how long an

organisation can retain record and be able to recreate those records. Selecting and deciding on the type of backup strategy for an organisation solely depends on their own backup policies and protocols the recovery site could be a worm site, hot site and cold site recovery location depending on the organisation needs and requirements. Data can be stored on site (which can be easily) recoverable and accessible to the organisation but in the event of failure, retrieving a media file from an alternate storage location will be impossible. Data backup can also be located in the offsite location which is expensive (payment to rental and services fees of location and services associated with) data storage furthermore the recovery site alternative can be a worm site, hot site and cold site.

4.1 Hot Sites

Hot site back up site that has duplicate of main site to the secondary site duplicate of your data stored, prepared for admission in an emergency scenario the pros of hot site backup site defeat data in the main site can be guaranteed to be recouped afterward a catastrophe but its expensive (cost of web traffic). According to Coreexchange (2015) a "proactive" hot site permits you to retain servers and a live backup site up and running in the event of a disaster. Basically, you replicate your creation environment in our data centre. This permits for an instant cutover in case of catastrophe at your main site. A hot site is a have to for duty critical sites.

4.2 Warm Site Backup

A "preventative" honest site permits you to pre-install your hardware and pre-configure your bandwidth needs. Then, if catastrophe strikes, all you have to do is burden your software and data to reinstate your company arrangements (Coreexchange, 2015).

4.3 Cold Site Backup

A "recovery" chilly site is vitally just data centre space, domination, and web connectivity that's prepared and staying for whenever you could demand it. If catastrophe strikes, our builder and logistical prop teams can effortlessly aid you move your hardware into our data centre and become you back up and running (Coreexchange, 2015).What's right for your firm depends on your budget, the sensitivity of your data, the number of chance you're keen to seize on, and the number of period you're able to take beforehand fully refurbishing your company operations. Contact us to discover extra concerning how a hot site, honest site or chilly site can aid safeguard your company's future.

4.4 Recovery Point Objective and Recovery Time Objective

Recovery Point Goal (RPO) and Regaining Period Goal (RTO) are one of the most vital bounds of a catastrophe recovery or data protection plan. These goals escort the enterprises to select a optimal data backup (somewhat restore) plan. Recovery Point Goal (RPO) describes the interval of period that could bypass across a disruption beforehand the number of data capitulated across that era exceeds the Business Continuity Plan's maximum allowable threshold or "tolerance (Singh, 2008). The Recovery Period Goal (RTO) is the period of period and a ability level that a company procedure have to be revamped afterward a catastrophe in order to circumvent undesirable aftermath associated alongside a break in continuity. In supplementary words the RTO is the answer to the question: "How far period did you seize to recovery afterward notification of company day to day activity disruption (Singh, 2008). However, at early scan these two words materialize to be quite similar. The best method to comprehend the variance amid them is to associate the "RP" in "RPO" by envisioning that they stand for "Rewrite Parameters" and the "RT" in "RTO" as "Real Time." RPO entitles the variable amount of data that will be capitulated or will have to be re-entered across web downtime. RTO designates the number of "real time" that can bypass beforehand the disruption begins to critically inadmissibly, obstruct the flow of regular company operations. The RTO/RPO and the aftermath of the Business Impact Analysis (BIA) in its entirety furnish the basis for recognizing and analyzing viable approaches for inclusion in the company continuity plan. Viable approach preferences should contain each that should enable recommencement of a company procedure in a period construction at or adjacent the RTO/RPO. This should contain alternate or guidebook workaround procedures and should not necessarily require computer arrangements to encounter the purposes. Figure 1.3 delineates the recovery period goal and recovery point objective.

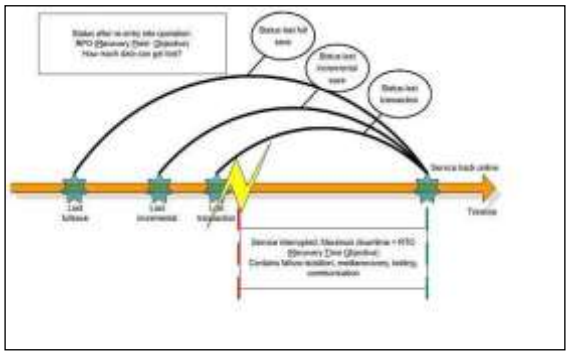

Figure 1.3: The recovery time objective and recovery point objective: Sources (Livens, 2015)

Figure 1.3 displays that RTO and RPO are critical metrics for today's data protection settings, and selecting the appropriate way needs a methodical understanding of the nature and company objectives. It is frequently functional to join resolutions to accomplish RTO and RPO necessities as grasping finished costs. A vintage example is employing oftentimes daily snapshots for short-term RPO and RTO as yet relying on maximum backups nightly for longer word retention. The maximum backups enable you to check the number of snapshots retained that can cut prices and nature complexity.

5. Existing Disaster Recovery Framework

This section highlights the existing disaster recovery planning proposed by different researchers with the sole aim of planning for disaster, responding to disaster and restoring systems to its previous state to ensure the continuity of business in any organisation. Thus, some researchers classified some of the disaster recovery phase activities as phases while some of them classified the phases as an activity. Table 1.1 illustrates the study conducted by researchers.

5.1 Disaster Recovery Plan Features

The implementation of the strategy will be based on best practice and standard will be possible for any organization to implement as its plan disaster recovery plan for any organization, here is detailed comparative analysis of existing features of disaster recovery models. Thus, as to ensure the proposed strategy for executing DRP activities will following best practice features and processes anticipated by different authors so as to meet organizations information security requirement and the continuity of their business pre and post disaster strikes be it manmade or natural. Table 1.2 illustrate some vital features anticipated by different authors and merging the features and processes of the existing DRP models and base on this features and there activities we are going to proposed the strategy.

Table 1.1 below shows the selection of the disaster recovery plan is derived from that analyses and maps the selection of phases required for the disaster recovery plan. The mapping of the phases is according to the existing study by researchers. The detailed selection is shown below:-

- Disaster Risk Assessment : 7 of 10 researchers
- Disaster Prevention : 6 of 10 researchers
- Disaster Preparedness : 6 of 10 researchers
- Disaster Response : 6 of 10 researchers
- Immediate Recovery : 9 of 10 researchers

Nonetheless, table 1.1 illustrates the lesson learnt is that all the features and mode of selection are generic and can be applied for any other disaster recovery but, the features nearly fit to disaster recovery. Nonetheless, in this research, some of the processes and activities will be generic to all types of disaster recovery but some portion (such as the recovery portion) is most critical to the organisation

The justification of the selected disaster recovery model is based stages, processes and techniques proposed by different authors. Thus, a comprehensive study on disaster recovery model and comparative analysis of the existing disaster recovery models are essential. The selection of phases of disaster recovery is based on the comparing and merging the stages and processes as well as selecting the best practice process that can be used by any organization based on their security needs and requirements. The proposed strategy for executing activities of the selected phases will comprise of the below named phases which includes the following: -

- Disaster Preparedness
- Disaster Risk Assessment
- Disaster Prevention
- Disaster Response
- Immediate Recovery.

Table 1.1 Feature Mapping of Disaster Recovery Plan features

	Features \ Authors	Snedaker (2013)	Gregg (2009)	NIST (2014)	ISO (2010)	Gilbert, S. W. (2010)	Sans, (2008)	Tuydes, H. (2005)	James K, (2011)	Whitman M., Mattord H., and Green A.,(2013)	Rittinghouse J. P. D. C. and P. D. C. C.JamesF.R.,(2011)
1	Project Initiation		✓	✓	✓						
2	Project Planning	✓	✓	✓	✓	✓	✓	✓	✓	✓	
3	Disaster preparedness		✓	✓	✓	✓			✓	✓	
4	risk Initiation	✓		✓	✓		✓	✓			
5	Risk assessment and evaluation	✓	✓	✓	✓	✓		✓		✓	
6	Develop Business Impact Analysis	✓	✓				✓			✓ ✓	
7	Develop BCP and management strategies	✓		✓	✓	✓	✓				
8	Emergency response and operations			✓	✓		✓	✓			
9	Identify risks			✓				✓		✓	✓
10	Protect against risks	✓		✓	✓	✓					
11	Respond to risks			✓	✓	✓	✓	✓			✓
12	Detect risks	✓		✓	✓		✓	✓	✓		✓

13	Mitigate risks				✓	✓	✓				✓
15	Disaster Response Team		✓	✓	✓					✓	
16	Immediate Disaster Recovery	✓	✓	✓	✓	✓	✓	✓		✓	✓
17	Createcontingency strategies		✓	✓	✓			✓		✓	✓
18	Develop IS contingency plan			✓	✓			✓			
19	Awareness and training		✓				✓			✓	✓
20	Disaster review	✓			✓	✓	✓				
21	Documentation and lesson learnt	✓		✓	✓			✓		✓	✓
22	Disaster identification and notification	✓	✓				✓				✓
23	Disaster response efficiency			✓	✓	✓		✓			
24	Backup procedures	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
25	Activating Disaster recovery plan	✓		✓	✓		✓		✓		✓
26	Facilitate monitoring control			✓	✓					✓	
27	Digital forensic support			✓	✓		✓				
28	Establish level of trust between entities	✓		✓	✓						
29	Development of Recovery strategies	✓		✓	✓					✓	✓
30	Steering Committee commitment to DRP development	✓		✓	✓						✓

31	Testing backup procedures	✓		✓	✓		✓			✓	✓
32	Disaster Recovery team	✓		✓	✓	✓	✓		✓		
33	translating strategies into plans			✓	✓						
34	incident response	✓		✓	✓					✓	✓
35	Offsite Storage Consideration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
36	Conducting BIA	✓	✓	✓	✓		✓			✓	
37	Emergency Backup		✓	✓							✓
38	Immediate Backup		✓	✓							
39	Document incident	✓	✓	✓		✓				✓	
40	Long Term Backup			✓	✓						
41	Off-Site Storage of Critical Supplies	✓	✓	✓							
42	Restoration to normalcy			✓	✓						
43	Develop the contingency planning policy statement	✓			✓						
44	Develop business continuity plan		✓			✓				✓	
45	Identify preventive controls	✓	✓	✓	✓	✓					
46	Ensure plan testing, training and exercise of DRP			✓	✓					✓	✓
47	Ensure plan maintenance			✓	✓					✓	

48	formulate a DR report	✓	✓		✓	✓				✓	✓

5.2 Extracted phases Activates

The research has extracted the most commonly used phases and activities from the literature and formulated a table that explain each phase with it corresponding activities. Table 1.2 below detail out the phases.

Table 1.2 Disaster recovery phase and their activities

Phases	Activities
Disaster Risk Assessment	• Identifying the risks to assets • Conduct threat assessment • Conduct vulnerability assessment • Determine threat potential impact on the key business process • Conduct risk mitigation strategy
Disaster prevention	• To know the main areas of risk and to take steps to minimise the risk or detect any problems as early as possible • to ensure that personnel are trained and prepared to play a positive role in preventing disasters • to know the asset and equipment storage areas well • to ensure good lines of communication with staff working in those areas • to ensure good lines of communication with other key staff likely to be involved in disaster prevention, response and recovery •
Disaster Preparedness	• Understand what data and systems are critical to business continuity • Establish damage assessment team and disaster recovery team • Create a workforce continuity plan • Create a disaster recovery plan • Train your staff on disaster response • Establish employee security training and awareness
Disaster Response	• Establish disaster emergency Response Team • Assessing the impact of threat and damages to business • Protect the asset from further damages • Notify or verify the notification of people and programs that are designated to respond in an emergency • Activation of emergency response checklists
Immediate Recovery	• Scanning for threat and vulnerability • Isolation and eradication threat form infected system • Recovery and prevention from data loss

6. Conclusion

The paper have explained a detailed breakdown of disaster recovery and it current phases and activities

widely adopted by many researcher, the paper has proposed phases from the literate an activities plan for further research execution. The extracted activities can be implemented for any organizational disaster recovery action plan.

7. Reference

[1] Anderson, R. 2009. Why information security is hard-an economic perspective. Computer Security Applications Conference, 2009. ACSAC 2009. Proceedings 17th Annual, IEEE.

[2] Whitman, M. and Mattord, H. 2013. Management of Information Security, Cengage Learning.

[3] Rouse, Margaret. 'What Is Hot Site And Cold Site? - Definition From Whatis.Com'. SearchCIO. N.p., 2015. Web. 26 Apr. 2015.

[4] Rothstein, P.J. 2007. Disaster Recovery Testing: Exercising Your Contingency Plan(2007 Edition): Rothstein Associates Incorporated\

[5] Snedaker, S. 2013. Business Continuity and Disaster Recovery Planning for IT Professionals, ElsevierScience.
http://www.itjungle.com/tfh/tfh072610-story10.html. Last accessed 10th Oct 2014.

[6] Woodie, A. 2010. Human Error the Number One Cause of Data Loss, Survey Says. [Online]Available: Solomon, M. G. 2013. Security Strategies in Windows Platforms and Applications, Jones.

[7] Wells, A. J., et al. 2006. Disaster Recovery: Principles and Practices, Pearson Prentice Hall.

[8] Corexchange, Inc. 'Disaster Recovery Hot, Warm, Cold Sites: Key Differences'.Corexchange.com. N.p., 2015. Web. 26 Apr. 2015.
Singh, Jaspreet. 'Understanding RPO And RTO - Druva'. Druva. N.p., 2008. Web. 26. Apr. 2015.

[9] Livens, Jay. 'The Criticality Of RTO And RPO | Siliconangle'. Siliconangle.com. N.p., 2015. Web. 26 Apr. 2015

[10] Woodie, A. 2010. Human Error the Number One Cause of Data Loss, Survey Says. [Online]Available: Solomon, M. G. 2013. Security Strategies in Windows Platforms and Applications, Jones.