Discretization of Disaster Recovery Choices: A Survey of Tier Schemes

Omar H. Alhazmi[*] and Yashwant K. Malaiya[†]

[*]Department of Computer Science, Taibah University,
Medina 30001, Saudi Arabia
ohhazmi@taibahu.edu.sa

[†] Department of Computer Science, Colorado State University,
Fort Collins, Colorado 80524, USA
malaiya@cs.colostate.edu

Abstract

Disaster recovery plans (DRPs) for IT systems have been around since the 1970s. Disaster recovery plans vary in their design, performance, goals and technologies used. Therefore, a need to classify disaster recovery plans into discrete tiers emerged. A number of tier schemes has been proposed and used; unfortunately, the tier levels used across schemes do not match making the classification confusing or inappropriate for the current state of technology. Moreover, it is often in the literature to find the same classification exists in different versions and in different terminology. The widely used classification of 7-tiers of DRPs which was appropriate for the 1990s is now obsolete. We survey alternative tier schemes that have been proposed since, in order to understand the common grounds and the differences and suggest desirable attributes of a discretized tier scheme.

Keywords: Disaster Recovery Tiers, Disaster Recovery, DRP, RPO, RTO.

1 Introduction

Processing and storing of information is inherently failure prone. Disaster recovery for data had emerged as a major technical field by late 1980s when the widely mentioned seven-tier classification was developed by the SHARE technical steering committee working with IBM. They developed a whitepaper that described levels of service for disaster recovery using Tiers 0 through 6. [1, 2]. The levels, “Tier 0” to “Tier 6” are discussed in detail in the IBM Red Book by Brooks et. Al [3]. The classification starts at “Tier 0” where there is no offsite data (i.e. no disaster recovery plan) going up to Tier 6 characterized with zero data loss level. Sometimes, a 7thTier is added that represents an integrated automated solution.

The terminology reflects the technology before widespread use of the internet; thus, Tier 1 involves “Pickup Truck Access Method” (PTAM) and Tier 3 is termed “Electronic vaulting”. Since then, the hard drive costs have dropped by factor of about 100,000, internet access is faster by a factor of ten thousand, and concepts such as virtualization and public cloud have become widely accepted.

Discretization is important because it allows an organization to choose among the available choices, without making the process complex. The SHARE/IBM scheme discretized the choices by the technologies available. Discretization can also be done by dividing the performance attributes into discrete ranges, or by the technical approaches used. Computer Network Technology proposed a 4-class scheme depending on *recovery point objective* (RPO) and *recovery time objective* (RTO) ranges [4], which are the two of the most important numerical attributes of a DRP. RPO is the maximum duration for which the incoming transactions can be lost. It thus depends of the duration between two successive instants when data is saved. RTO is the time during which the system is undergoing recovery and is thus not available. Schemes proposed include Hitachi’s 9-levels of protection sand 5-tiers disaster recovery scheme [5], Xiaotech’s [6] 4 tier scheme and Novell’s 5-tiers [7] scheme.

Emergence of virtualization and cloud computing have dramatically changed how disaster recovery planning is done now [8], they add new parameters to costs and disaster recovery efficiency by incorporating cloud computing technology in disaster recovery. Recently Firdhous [9] has proposed a scheme for cloud disaster recovery service model (DRaaS) consists of 3 categories (Hot, Warm and Cold).

Studies show that disaster recovery cost is a main factor why many organizations choose not to acquire the best disaster recovery solutions. A solution consisting of multiple criticality level and disaster recovery tiers can

978-1-943436-02-6 / Copyright ISCA

reduce the cost and make it more affordable (higher tiers for the critical parts and lower tiers for the non-critical parts of the system) [10].

Organizations need a descriptive scheme that can represent the technological alternatives available today. We ask the questions - Is the classical seven tier still applicable today? Can the proposed DR tier schemes be correlated with each other? Do we need a new way to discretize the disaster recovery choices?

This work aims at providing an independent study of existing classification schemes and explores the possible option to reconciling them among themselves and with the current technology. We discuss new factors and their implications, and then we recommend new enhanced framework for classifications of disaster recovery plans to make it easier to identify and evaluate the possible DRPs.

Here, we investigate several multi-tier DRPs and propose a new scheme that should provide an appropriate systematically defined framework for planning disaster recovery. It is flexible enough to allow for future technological advances in near future. The paper will discuss major differences and similarities among different existing disaster recovery schemes. It will also look the potential RTO, RPO [11], the distance between the primary and the backup systems [12], the probability of a failed recovery and finally the cost/ROI aspects of the choices. Then we propose a new framework for disaster recovery classifications which gives clear distinction between different tiers and covers new improvements in technology and the new factors and parameters in the environment.

In the next section we shall overview some of the most well-known disaster recovery schemes in detail; then in section 3 we will discuss these schemes, and in section 4 we will give a conclusion and some future research directions.

2 Overview of Disaster Recovery Tiers Schemes

Here we discuss the following different schemes that have been around since the late 1980'. The chronology is shown in Figure 1 below:

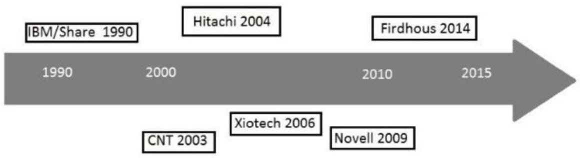

Figure 1- The timeline for some DR schemes

In the following sub section, we will give a brief description of each scheme.

2.1 IBM/SHARE scheme:

Table 1 below shows SHARE/IBM scheme which is one of the earliest (1990) and still the most mentioned DR tier scheme. It reflects the technological choices available then. Table 1 describes each disaster recovery tiers including the tier with no DR plan (i.e. tier 0). Then tier 1, which represents the basic regular "manual" backup solution, also referred to as Pick-up Truck Access Method (PTAM). Tier 1 has low cost and can be ideal solution cost-wise for individuals, small organizations and non-critical business data. Alternatively, tier 2 follows the same concept with an important addition of standby ready-to-go system. For both tier 1 and tier 2, RTO and RPO requirements should be relaxed considered high ranging from hours to days and the main technology considered is tapes backup.

Table 1- SHARE / IBM Disaster Recovery Tiers

Tier	Technology	Description
0	No off-site data	No saved information, no recovery plan at all
1	Data backup with no hot site (PTAM)	Data are packed up and taken to a remote location for storage, also called PTAM; *the "Pick-up Truck Access Method."*
2	Data backup with a hot site	Same as tier 1; however, the remote site has ready infrastructure capable of restoring operation to the latest backup within hours/days
3	Electronic vaulting	Same as tier 2; however, backups are done via electronic vaulting, and high speed communication (no PTAM)
4	Point-in-time copies	Same as tier3; however, data are backed up more frequently; thus, better estimation of data loss and recovery time.
5	Transaction integrity	This application level tier ensures that original site and backup site are consistent; thus, minimizing loss to zero or near zero level.
6	Zero or little data loss	This tier requires site mirroring, two sites working in sync
7	Highly automated, business integrated solution	Same as tier 6; plus the recovery process is automated; therefore, the system will recover itself with no or minimum intervention.

Beginning from tier 3 and up, will be having a disaster recovery with predictable more precise RTO and RPO; so, tier 3 has some of the critical data stored on disks rather than on tapes, thus reducing recovery time objective. At tier 4, a complete image is taken frequently significantly reducing both RPO and RTO over tier 3. However, at tier 5 the disaster recovery moves from just backups to the two active sites: primary and recovery. Integrity is maintained on transaction level; thus, requiring application level support. One step up is tier 6, which requires synchronization of primary and recovery sites. In both tier 5 and 6, RTO improves from hours and days to minutes and seconds. On the other hand, RPO improves to losing few transactions or even zero data loss. Moreover, tier 7, is reserved for fully automated solution with disaster detection and recovery with minimum human intervention.

2.2 Hitachi Disaster Recovery Scheme:

Hitachi has defined two disaster recovery schemes one with five tier levels [5] (Table 2) and the other with 9 levels of protection [5].

Hitachi's tier 5, is "three-data-center" tier, involves having three data centers, an original site, a local secondary site connected synchronously with the original; thus, the lag should be minimal. Additionally, a third remote secondary site connected asynchronously with the original. This tier combines the benefits of tiers 3 and 4.

Note that *synchronous replication* involves making changes to both sites at the same time, whereas in *asynchronous replication*, the backup is updated after some delay.

First, by looking at Table 2 we can see that Hitachi's tier 1 is referring to using tape while tier 2 is using disk. However, Hitachi's tier 3 involves having two sites working together in sync while after each transaction the original site will wait until the secondary site will make sure transaction is completed, this can be helpful; however, the main drawback is that is the lag especially when the sites are located at significant distance. Therefore, tier 4 suggests an asynchronous solution where the secondary site receives new data along with timestamp, so without causing delay to the original site the secondary site will be updated, this is especially recommended for sites located remotely from each other which is ideal when a natural disaster affects certain geographical area.

Table 2- Hitachi Disaster Recovery Tiers

Tier	**Technology**	**Description**
1	Tape Backup	Data are packed up in tape and taken to a secure location
2	Disk Point in Time Backups	Data are packed up on disk frequently
3a	Synchronous	Original site waits for the secondary site to replicate each transaction
3b	Sync with Failover	Same as above with failover capability
4a	Asynchronous	The original site continue to works normally while the secondary site track of pending transactions and make sure they get processed
4b	Async with Failover	Same as above with failover capability
5	Three Data centers	Combines the synchronous technique for a local secondary site and an asynchronous remote site

Hitachi's tier 5, is "three-data-center" tier, involves having three data centers, an original site, a local secondary site connected synchronously with the original; thus, the lag should be minimal. Additionally, a third remote secondary site connected asynchronously with the original. This tier combines the benefits of tiers 3 and 4.

Table 3- Hitachi Levels of Protection

Level	Level Name	Description
1	Tape Backup (offsite)	Data are packed up and taken to a remote location for storage, also called PTAM; *the "Pick-up Truck Access Method."*
2	Tape Backup (onsite)	Same as tier 1; however, the remote site has ready infrastructure capable of restoring operation to the latest backup within hours/days
3	Electronic Vaulting	backups are done via electronic vaulting, and high speed communication (no PTAM)
4	Single Disk Copy	Data are backed up more frequently; thus, better estimation of data loss and recovery time.
5	Disk Consolidation	Centralized data storage
6	Shared Disk	All nodes share all disks
7	Disk Mirroring	Typically synchronous approach
8	Remote Disk Mirroring	Can be synchronous or asynchronous
9	Complete Duplication	Two or more identical systems with identical specifications

Hitachi also uses "9-levels of protection (Table 3)"which has levels 0 to 4 identical to its counterpart of IBM/SHARE's tiers (see Table 1). Then at tier 5, high level DR solution is employed by using disk consolidation which requires operating system and/or application level support. Furthermore, level 6 includes using a pool of disks; then at level 7 will require full mirroring where all transactions must be completed in parallel in both primary site and recovery site. Then, at level 8, two remotely located sites must run in synchronously or asynchronously. Finally, a level 9 requires a complete duplication of the whole system.

2.3 Xiotech scheme

In 2006 [6], Xiotech revisited the 7-tier system and they have proposed their 4-tier classification shown in Table 4. They have discussed the 7-tier system indicating that the solutions can be categorized into two main categories. First, the *PTAM* category solutions group which is generally low cost solutions with non-strict RPO/RTO requirements and do not need special customized hardware or software. Second, the *Glasshouse* solutions group which is higher in cost, it satisfies the need of critical business with dedicated software and hardware for disaster recovery purposes and the result would be strict RPO/RTO requirements.

Xiotech has introduced simplified version that can reduce the number of tiers to only four. Also, they relate their tiers to IBM/SHARE tiers as shown in Table 4 .Their tiers classification appears to be customized for business and marketing purposes; which can be easily fit with a Service Level Agreements (SLAs).

Table 4-Xiotech Disaster Recovery Tiers

Tier	Technology	Description	Comparable IBM/SHARE Tiers
1	**Instant Recovery** (Hot Site)- Synchronous Replication	Mission critical	Tiers 5/6
2	**Rapid Recovery** (Hot Site)- Asynchronous Replication	Mission critical/business vital	Tiers 4/5
3	**Fast Recovery** (Warm Site)- Asynchronous Replication or scheduled replication	Business vital/ business important	Tiers 3/4
4	**Standard Recovery** (Cold Site)-Scheduled Synchronous Replication	Business important/ important for productivity	Tiers 2/3

Xiotech classification starts at tier 1 which is the highest and has the lowest RPO and RTO, this tier is said to be comparable to tiers 5 and 6 of the IBM/SHARE classification, then comes tiers 2, 3 and 4 which is the lowest. At tier 4 here we notice that this classification does not include a level compared to tier 1 of IBM/SHARE system which can be understandable because Xiotech classification is more recent and focused on the higher level.

2.4 Novell scheme

Originally, Novell used a 4-tier scheme, and then they pointed out that there is a gap in cost between “flexible imaging” and “server clustering” tiers (Table 5). Thus, they proposed adding the “tier 4, consolidated recovery using virtualization” to bridge the gap and to have a level with intermediate cost and performance; this made Novell scheme a 5-tier scheme (2009) [7].

Table 5- Novell Disaster Recovery Tiers

Tier	Technology	Description
1	Tape Backup /Manual System Rebuild	Use tapes to store data, recovery done manually
2	Traditional Image Capture	Frequent scheduled capture of system data
3	Flexible Imaging	
4	Consolidated Recovery using Virtualization	
5	Server Clustering	A set of servers working together, work continue even if one server fail

2.5 Computer Network Technology scheme

In the CNT (Computer Network Technology) classification [4], a two dimensional classification has been proposed as shown in Table 6.

The classification separates the two factors RPO and RTO; therefore, one can have a class 1 RTO and class 2 RPO system and so on.

Table 6- CNT DR tiers Scheme

	Class 1	Class 2	Class 3	Class 4
RTO	72 Hours - 1 Week	8 - 72 Hours	Less than 8 Hours	0 Minutes
RPO	Last full backup - Less than 1 Wk	Last Backup - less than 24 Hrs	Less than 15 Min. before the Event	0 Minutes

2.6 Firdhous classification

Firdhous in his recent comprehensive taxonomy (2014) for cloud computing services has disaster recovery as a service (DRaaS) and its advantages; basically, he classified DRaaS into three levels cold (CDDRaaS), warm (WMDRaaS) and hot (HTDRaaS) as given in Table 7, below [9]. However, Firdhous has not given further details about the factors used to classify a certain DRaaS into one of the categories.

Table 7-Firdhous classification [9]

level	Disaster Recovery as a Service levels
1	Cold site (CDDRaaS)
2	Warm site (WMDRaaS)
3	Hot site (HTDRaaS)

3 Discussion

Let us take a close look at those major disaster recovery classification schemes. The existing schemes are compared in Table 8. Different schemes have looked at the DRPs from different prospective. While some of them focused on how DRPs are built and the technology used (e.g. IBM/SHAREs, Novell), others consider how the original site is connected with the remote site (e.g. Hitachi), while the classification by Xiotech and CNT looks at the overall performance as required by the user as defined by RTO and RPO constrains.

As for the number of tiers it is getting fewer for the newer classifications and the main reason is that the lower tiers DRs are primitive and thus not discussion about it in the business and this can be a valid point to exclude them from classifications.

These classifications although they don’t contradict with virtualization and cloud; they do not directly address virtual or cloud DR except for Novell and Firdhous. Thus, there is a need to refresh these classifications in order for them to fit cloud and virtualization in them.

One important issue is separation of RPO and RTO, only CNT distinguish and give separate rating for each one. This is especially important when RPO and RTO are not equally important to a certain organization. For example, for a communication tower returning to operation is much more important than recovering lost data. On the other hand, for a billing system data loss is not tolerated and RPO is more important. Therefore, separating RPO and RTO is very important in some cases and we can see the CNT did well in this area.

Table 8-Overview of the 7 classification

Scheme	Direct Support of virtualization	Number of Tiers	Dimensions	Total
IBM/ SHARE	No	8 Tiers	1	8
CNT	No	4 Classes	2	8
Hitachi	No	5 Tiers	1	5
Hitachi levels of protection	No	9 Levels	1	9
Xiotech	No	4 Tiers	1	4
Novell	Yes	5 Tiers	1	5
Firdhous	Yes	3 Classes	1	3

For the older schemes, they need to reflect the new advances in storage and communication technology; since, the rise of virtualization and cloud computing DR systems are becoming more affordable than ever. Here, the schemes can play good role in simplifying DRaaS billing as customers can set there RPO and RTO constrains and can easily compare among different DRaaS providers.

Finally, the ideal classification would be a two dimensional scheme that separates RPO and RTO similar to CNT; moreover, the scheme should also consider cloud and traditional disaster recovery systems.

Discretization is a common technique to simplify classification of attributes or choices. With wide availability of internet and cloud technologies and market competition, the market represented by the services provided has become efficient with the cost becoming a function of the services provided. The continuous attributes RPO and RTO, along with a few other (for example the probability of unrecoverable loss, scalability for large amounts of data (big data), and predictability of performance) thus are emerging as suitable choices of factors that can be discretized [13] [14].

Choice of discretization levels can be based on dividing lines that are in some way natural, perhaps representing the limits of cost effectiveness of technical choices. Alternatively, they can be guided using round numbers. The division of levels can be linear, although often it makes more sense for them to be exponential (with linearity after taking a logarithm).

Technology has progressed steadily. Technological hurdles (such as processor clock frequency) are generally bypassed by new developments. Storage costs have steadily dropped and the emergence of 3D Xpoint promises much faster speeds and eventually lower costs. Data transfer rates have also been going up and the associated costs have been dropping. It would be convenient if the tier levels are developed with can be easily adapted to technological advances can be forecasted in near future.

Only limited studies have been done on analytical modeling of DR attributes and associated costs. Further studies need to be undertaken so that they can guide the development of ideal DR tier level schemes.

4 Conclusion

We have reviewed a number of disaster recovery schemes, they help us understand the capability of the DR system and how to differentiate among different disaster recovery systems alternatives. We have discussed these schemes from the aspect of technology, modernity and other aspects. We have noticed that most of the classifications available today are developed by the leading names in industry, especially industries building storage systems; however, we have seen that academic research are becoming more interested in disaster recovery systems and technology.

Further studies are needed to suggest robust classifications that can be more accurate and vendor-independent and can be widely accepted by industry and academia, which can give organization better prospective on what kind of DRP they can afford and what performance level they can expect from it. Furthermore, a better classification can lead to identification of underlying techniques that will be quantitatively shown to be most effective for disaster recovery systems.

We can conclude that the existing approaches need to be updated and they need to be more flexible, quantitative and clearly defined.

References

[1] Robert Kern, Victor Peltz, “Disaster Recovery Levels”, IBM Systems Magazine, November 2003.

[2] Recovery Specialty LLC, “Business Continuity: The 7-tiers of Disaster Recovery”, http://recoveryspecialties.com/7-tiers.html, 2007.

[3] C. Brooks, M. Bedernjak, I. Juran, J. Merryman, Disaster Recovery Strategies with Tivoli Storage Management, IBM/Redbooks, November 2002,

http://www.redbooks.ibm.com/redbooks/pdfs/sg246844.pdf

[4] CNT, Alternate Site Recovery Techniques. White Paper. 2003.

[5] Roselinda R. Schulman, Disaster Recovery Issues and Solutions, A White Paper, Hitachi Data Systems, September 2004.

[6] Tiered Data Protection and Recovery, Xiotech Corporation, May 2006.

[7] Novell, “Consolidated Disaster Recovery”, http://www.novell.com/docrep/2009/03/Consolidated_Disaster_Recovery_White_Paper_en.pdf, March 2009.

[8] T. Wood, E Cecchet, K. K. Ramakrishnan, P. Shenoy, J. van der Merwe, and A. Venkataramani, “Disaster recovery as a cloud service: economic benefits & deployment challenges”, Proc. 2nd USENIX Conference on Hot topics in cloud computing (HotCloud'10), Berkeley, CA, USA, 2010.

[9] Firdhous, M., "A Comprehensive Taxonomy for the Infrastructure as a Service in Cloud Computing," in the Fourth International Conference on Advances in Computing and Communications (ICACC), 2014, pp.158-161, Kochi, India, 27-29 Aug. 2014.

[10] John Bullitt, “Develop a multi-tiered disaster recovery Strategy”, http://www.cambridgecomputer.com/PDF/0309isBullitt.pdf, accessed 2013.

[11] Akshat Verma, Kaladhar Voruganti, Ramani Routray, and Rohit Jain. 2008. SWEEPER: an efficient disaster recovery point identification mechanism. In Proceedings of the 6th USENIX Conference on File and Storage Technologies (FAST'08), Berkeley, CA, USA, pp. 297-312.

[12] T. Wood, H. A. Lagar-Cavilla, K. K. Ramakrishnan, P. Shenoy, and J. Van der Merwe. Pipecloud: using causality to overcome speed-oflight delays in cloud-based disaster recovery. In Proceedings of the 2nd ACM Symposium on Cloud Computing, SOCC ’11, pp. 17:1–17:13, New York, NY, USA, 2011.

[13] Kishor S. Trivedi , Ruofan Xia, Quantification of system survivability, Telecommunication Systems, December 2015, Volume 60, Issue 4, pp 451-470.

[14] Levitin, G.; Xing, L.; Zhai, Q.; Dai, Y., "Optimization of Full vs. Incremental Periodic Backup Policy," in , IEEE Transactions on Dependable and Secure Computing, no. 1, pp. 1.