Are the Classical Disaster Recovery Tiers Still Applicable Today?

Omar H. Alhazmi
Dept. of Computer Science, Taibah University
Medina, Saudi Arabia
ohhazmi@taibahu.edu.sa

Yashwant K. Malaiya
Dept. of Computer Science, Colorado State University
Fort Collins, Colorado, USA
malaiya@cs.colostate.edu

Abstract—As disaster recovery plans (DRPs) for IT systems have been improving over the past decades; some metrics became widely accepted such as recovery time objective (RTO) and recovery point objective (RPO). However, disaster recovery plans and solutions vary in their design, sophistication and their required RTO/RTO. Therefore, a need to categorize disaster recovery plans into tiers has become necessary. Fortunately, a number of classifications exist but sometimes they are not fully explained; so, independent researchers may find the classification confusing or inappropriate for the current state of technology with significant overlap among tiers. Moreover, advances in communication and technology and the introduction of disaster recovery as a service (DRaaS) by several cloud service providers (CSPs) has reshaped the area of disaster recovery and development of DRPs. Therefore, one can argue that the old classification of 7-tiers of DRPs is obsolete and a new classification is needed. Here, we try to survey these classifications, understand the common grounds and the differences and try to suggest some improvements to gap them.

Key Words- Disaster Recovery Tiers, Disaster Recovery, Risk Analysis and Management, RPO, RTO

I. INTRODUCTION

The most widely used seven-tier classification was developed in late 1980s by 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 is also [3]. The classification starts at "Tier 0" where there is no disaster recovery plan going up to Tier 6 characterized with zero data loss level. Often, a Tier 7 is added to represent an integrated automated solution. The terminology reflects the technology before widespread use of the internet and with outdated terminology; for example, Tier 1 involves "Pickup Truck Access Method" (PTAM) and Tier 3 is termed "Electronic vaulting". Since 1990, 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 become familiar. Hitachi has used a slightly different tier scheme [4] (see Table 1). Recently, some modern schemes were

proposed; for example, the 7-tier scheme of Wiboonratr and Kosavisutte (W-K) [5] and the scheme of Xiaotech [6] which uses a simplified 4 tier scheme. Also, yet another classification was proposed by Novell with only 5-tiers [7] (see Table 1). A study by Wood et. Al. shows that improvements in virtualization and cloud computing has already changed how disaster recovery planning is done [8], this adds new parameters to costs and disaster recovery efficiency by incorporating cloud computing technology in disaster recovery and the term disaster recovery as a service (DRaaS) was introduced .

To optimize cost and efficiently allocate resources a multi-tiered disaster recovery system can be a viable choice by mixing different tiers according to their criticality [9]. For such DR systems, it is needed to have a descriptive scheme that can represent the technological alternatives available today. We ask the question -Is the classical seven-tier still applicable today? Can it be related to the choices available today?

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. Then we recommend a new enhanced framework for classifications of disaster recovery plans to make it easier to identify and evaluate the possible DRPs.

Here, we propose a new framework for disaster recovery classifications which gives clear distinction between different tiers and covers new technology and the new parameters in the environment.

II. DISASTER RECOVERY TIERS SCHEMES

Table 1 shows the five schemes side by side. All these schemes are comparable except for Xiaotech which shall be discussed later. For the first four schemes, at tier 1: Share/IBM, Hitachi and Novell define this tier as "tape backup", while at WK scheme is specified as point in time (PiT). Next, at tier-2: Share/IBM adds a hot site, while Hitachi adds an onsite backup, WK adds a provisional backup, and Novell adds manual image capture. When looking at tier-3, more automated "electronic vaulting" is used in both Share/IBM and Hitachi; however, Novell upgrades to flexible imaging, while WK make more frequent PiT capture at this level.

When looking at Tier 4 at Novell's scheme the gap start to build up when the sophistication increases at "Consolidated Recovery using Virtualization" level; this tier needs to be implemented on the operating system/disk management level. Actually Novell tier 4 is equal to tier 5 of the other schemes. On the other hand, tier 4 of Share/IBM and Hitachi is still a low level solution with typical backup, while WK adds remote logging. At tier 5, Share/IBM, Hitachi and WK solution is based on operating system/ disk management level. Moreover, Hitachi's tier 5, is "3-data-center" tier, involves having three data centers, an original site and local secondary site connected synchronously with the original; thus, the lag should be minimal. On the other hand, this is the "server clustering" top tier of Novell. Additionally, At tier 6, Share/IBM is defined broadly "zero or little data-loss", while Hitachi and WK point to adding more sophistication and capabilities.

TABLE I.   DISASTER RECOVERY TIERS

Tier	SHARE/ IBM	Hitachi	W-K	Novell	Xiaotech
0	No DRP				
1	Data backup with no hot site	Tape Backup (offsite)	Point in Time	Tape Backup /Manual System Rebuild	Tier4: Scheduled Synchronous Replication- Standard Recovery (Cold Site)
2	Data backup with a hot site	Tape Backup (onsite)	Tape to Provisional Backup site	Traditional Image Capture	
3	Electronic vaulting	Electronic Vaulting	Disc PiT copy, Multi-Hop	Flexible Imaging	Tier 3: Fast Recovery (Warm Site)- Asynchronous Replication or scheduled replication
4	Point-in-time copies	Single Disk Copy	Remote Logging	Consolidated Recovery/ Virtualization	
5	Transaction integrity	Disk Consolidation	Concurrent ReEx (RRDF, E-Net)	Server Clustering	Tier 2: Rapid Recovery (Hot Site)- Asynchronous Replication
6	Zero or little data loss	Shared Disk	Remote Copy		
7	Highly automated	Disk Mirroring	Remote Copy with Failover		Tier 1: Instant Recovery (Hot Site)- Synchronous Replication
8		Complete Duplication			

At tier 7 and 8 (in case of Share/IBM), disaster recovery system at these tier are completely mirrored with state of the art recovery, synchronization and failover and also disaster detection capabilities. Here, it is not defined precisely to give room for future technology and innovations.

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.

Almost all these classification combine RPO and RTO requirements within each tier; recently, there was a suggestion to separate RTO and RPO when looking at disaster recovery [10].

III.   CONCLUSIONS

Most of the classifications exists today are developed by the leading names in industry, especially industries building storage systems. Having an effective standard disaster recovery tiers will give industry a unified vision to look at disaster recovery and business continuity systems. Therefore, further studies are needed to suggest robust classifications that can be more accurate and vendor-independent and can be widely accepted.

We can conclude that older approaches need to be updated by separating RPO and RTO and have a matrix-like classification that will make it meaningful and flexible.

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] Roselinda R. Schulman, Disaster Recovery Issues and Solutions, A White Paper, Hitachi Data Systems, September 2004.
[5] Montri Wiboonratr and Kitti Kosavisutte, "Optimal strategic decision for disaster recovery," Int. Journal of Management Science and Engineering Management, V ol. 4 (2009) No. 4, pp. 260-269.
[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, pp. 8-8.
[9] John Bullitt, "Develop a multi-tiered disaster recovery Strategy", http://www.cambridgecomputer.com/PDF/0309isBullitt.pdf, accessed 2013.
[10] Seacliff Partners International,"what does data loss mean to you", http://seacliffpartners.com/wordpress/?p=706, August 2011.