Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2007 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2007

Portfolio-Based Approach for Disaster Recovery Planning for IT

Kanapaty Pelly Periasamy
Nanyang Technological University, Singapore, apelly@ntu.edu.sg

Charissa Mei-Ling Lim
Nanyang Technological University, Singapore

Tan Ngee Wei
Nanyang Technological University, Singapore

Michelle Qiuyin Xie
Nanyang Technological University, Singapore

29. Portfolio-Based Approach for Disaster Recovery Planning for IT

Kanapaty Pelly Periasamy
Lim Mei-Ling, Charissa
Tan Ngee Wei
Xie Qiuyin, Michelle

Nanyang Business School
Nanyang Technological University
Singapore 639798
apelly@ntu.edu.sg

Abstract
With the integration of IT with business operations and management, organizations are vulnerable to a myriad of threats ranging from computer viruses to natural disasters and deliberate acts of sabotage. Consequently, IT disaster recovery has emerged as a critical organizational issue. This paper proposes an application portfolio-based framework for IT disaster recovery planning based on the role of IT and the consequence of IT disaster. The findings and recommendations of the paper are based on interviews with disaster recovery experts and senior IT professionals and a case study.

Key Words: IT role, IT risks, disaster recovery, application portfolio

Introduction

The events of 9/11 have raised global consciousness on terrorism and the quantum of devastation that could be inflicted by such a dastardly act. While thousands of people and property perished in this pivotal point in modern history, only IT survived though it too was decimated – an oxymoron but true, thanks to the comprehensive disaster recovery planning (DRP) for IT that had been put in place by the firms which were affected. For example, Merrill Lynch's DRP enabled the renowned brokerage firm to successfully resume critical business functions within minutes after the 9/11 attack [Ballman, 2001]. 9/11 caused every major firm to review DRP arrangements and examine their adequacy – e.g. after 9/11, Price Waterhouse Coopers adopted a more comprehensive DRP covering all its offices across the globe [McCarthy, 2004]. The December 2004 tsunami in the Indian Ocean and the December 2006 devastating floods in Jakarta and parts of Malaysia were other notable wakeup calls, particularly for organizations in Asia, about the need for DRP for IT.

There was another major DRP impetus prior to 9/11 – the Y2K bug. The millennium bug issue increased organizational awareness of business disruption from IT failure and provided a big boost to DRP in the late 1990s. In addition to these wake-up calls and needs, DRP is also being driven by the "rapidly changing and growing risks from globalization, e-commerce and cyberspace, increased pace of business activities and international political risks" [Alonso et al., 2001], the Sarbanes-Oxley Act of 2002 (http://www.aicpa.org/sarbanes/index.asp) and business issues such as the increase in premiums charged by insurance companies for organizations that cannot demonstrate adequate disaster recovery capabilities [Hood, 2005].

Organizations are progressing from integration to fusion of IT with business. Such an arrangement, while being able to deliver optimal value, does have potentially heavy consequences - when a system crashes or is destroyed in a disaster, it may not be just a matter of business disruption but could be the kiss of death for the organization. Gartner estimates that two out of five enterprises that experience an IT disaster will go out of business within five years of the event because of inadequate DRP [Scott and Browning, 2002]. It is apparent

that DRP is a critical organizational issue in today's environment. This paper investigates DRP practice through literature review and field work, and proposes a portfolio-based approach for effective DRP practice.

Understanding Disaster Recovery Planning

DRP is concerned with reconstructing information systems and retrieving data when a primary facility of a business is damaged or destroyed [ABA, 2002]. Viewed more broadly, it could also embrace the IT infrastructure and facilities for hosting the systems and data. It is an organizational management activity conducted as part of Business Continuity Planning (BCP*)*, the arrangement of methods and procedures that enable an organization to respond to business disruption, ensuring mission-critical business functions and activities to continue in a planned and rehearsed manner. Essentially DRP is about ensuring the continuity of an information system when it is destroyed while serving the needs of an organization. For that to be possible, the two essential components which need to backed up and ready to kick in on a new host are the data and application software. Complementing these two would be related system configuration, documents and controls and procedures.

DRP involves a number of key steps:

- Form DRP Team and Steering Committee - The DRP team consists of senior executives from the IT department with specific responsibilities for data center operations, data management, application development/maintenance, planning/ architecture, etc. The DRP steering committee should have at least one representative from each business area and include executive management to "make the organization's leaders aware of the cost of lost business and the likelihood that the entire business will be lost" [Brunetto and Harris, 2001; Maiwald and Sieglein, 2002].
- Risk Analysis and Business Impact Analysis - The business assets, threats and impacts, as well as risks that can be tolerated need to be determined [Nosworthy, 2000]. Managers and personnel from various departments are interviewed to gain an understanding of the business model and mission-critical activities and the people, processes, and systems that support them. The organization then prioritizes them in terms of their role in reviving operations. The relative value of assets such as applications and data are assessed along dimensions such as the degree of connectedness and the need for availability [Cougias et al., 2003].
- Develop Recovery Strategies - The cost of recovery is influenced by the organization's recovery time objective (RTO) and recovery point objective (RPO). Develop IT security measures, as well as anticipatory and mitigatory strategies such as backup sites and duplex set-ups.
- Implementation, Testing and Training - The organization's employees must be trained in the disaster recovery procedures and tested to ensure that everyone is capable of carrying out their roles smoothly [Cerullo and Cerullo, 2004].
- Periodic Audit and Review - As an organization's situation and environment do not remain static, it is necessary for it to carry out periodic audits, reviews and drills of BCP and DRP [Morganti, 2002].

The planning process needs to be comprehensive and cover all relevant aspects and factors:

- Types of disasters which need to be addressed - from accidents, blackouts, fires, sabotage and terrorist acts to natural calamities such as earthquakes and floods.

- Business activities and needs of the organization – the critical business processes and activities which are reliant on IT; other business processes and their extent of dependence on IT
- Essential IT services - the data and application software that need to be recovered and restored for the business to resume in case of a disaster; other IT services needed to continue proper functioning in the event of a disaster (e.g. procedures and competences).
- IT infrastructure - the infrastructure (hardware, network and system software) needed to host the application software and data.
- Strategies and implementation arrangements - DR site arrangements and baseline strategies like main data centre facility protection, backup and IT security to guard against common place threats
- Challenges and emerging threats - new threats such as terrorism.

The Research Model

While there is abundant literature on DRP, research in this critical topic is somewhat limited. A study was hence conducted to research DRP and to offer insight for effective practice. The research model shown in Figure 1 was developed for this purpose.

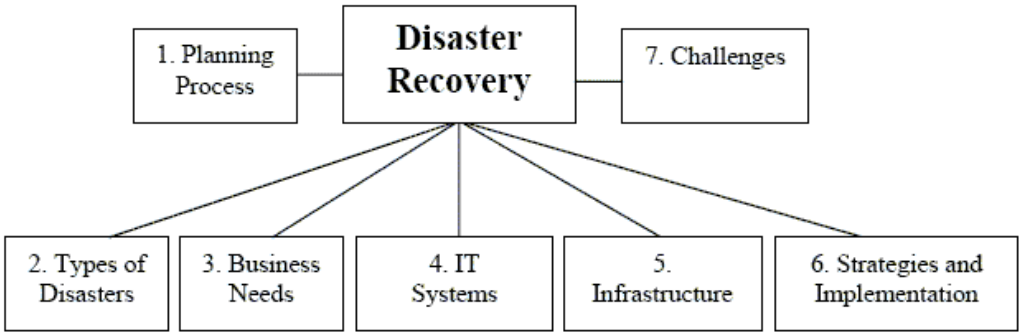


Figure 1: Research Model

The following questions were defined to complement the research model in the study:

- Why is DR needed in an organization?
- What preparations are needed?
- What are the components of DR?
- What are the challenges that organizations face in DR?

As the study touched a sensitive organizational issue and data might not be easily available, a multi-pronged approach was taken:

- Preliminary discussions with DRP practitioners
- In-depth case study on DRP
- In-depth interviews with DRP experts and DR site visits

Preliminary Discussions

In order to adequately prepare for in-depth case study work, background information and research pointers were gathered through participation in Singapore Computer Society's Business Continuity Group's events (e.g., "Recovery Strategies for Communications", Sept.

2004) and discussions with Gary Teo (Asst. Director, IT Services, Nanyang Technological University) and Geoffrey Khoo (Operations Manager, Singapore Computer Systems Ltd.).

Case study: National Library Board (Singapore)

Case study was chosen as the primary research technique as it is an effective method to gain insight into an issue lacking rich information. Organizations approached were very cautious about participating in the study as they viewed DRP to be an extremely sensitive and confidential topic. The Singapore National Library Board (NLB), a very successful exploiter of IT, nonetheless agreed to serve as a case study for this research.

The NLB (www.nlb.gov.sg) in recent years has been transformed into a state-of-the-art public library using IT to provide world-class library services on a 24x7 basis. The scope of NLB's operations includes extensive use of IT for handling the loan of books and other items, online delivery of e-books/magazines/databases, and operating and managing the library and its online services. DRP has emerged as a top priority in NLB, given the fusion of IT with its operations and management.

Background information was obtained from NLB's publications. NLB'a website was visited to learn about the organization. Published literature, such as "Transforming Singapore's Public Libraries" by Hallowell et al. [2001] (Harvard Business School case study), were studied. A few of NLB's libraries were visited to observe activities and services. The websites of vendors who provided the library's backend systems were visited. All this preparatory effort proved invaluable during the field work.

During the case study process, relevant reports such as NLB's Disaster Recovery Project Management Plan and the manual for eLibraryHub (NLB's digital library service) architecture were examined to understand NLB's IT functions and systems. NLB's primary DR site was visited to observe and learn about ongoing DRP activities. The following key executives were interviewed on specific DR issues and topics:

- Lau Kai Cheong, CIO
- Kuan Sung, Senior Manager of Operations, IT Division
- Ling Min Chin, Assistant Director of Application Integration
- Alan Chong, Manager, IT Division
- Michael Fu, ELH System (a key application IT Division) Owner
- David Hong, Consultant, National Computer Systems Pte Ltd (NCS) - vendor
- Nazhath Sultana (Ms.), Senior Systems Engineer, NCS

In-depth Interviews

In order to gain further insight and discuss findings from the case study, the following DRP experts were interviewed in the next stage of field work:

- Goh Moh Heng (Dr.), Director of DRI Asia (a major disaster recovery organization)
- Annie Phang (Ms.), Honorary Secretary, Executive Council of Business Continuity Group, Singapore Computer Society
- Wong Tew Kiat , Senior. Manager, Business Recovery Centre, SCS Ltd. (vendor)
- Michael Hii, Marketing Manager, Singapore Telecom, EXPAN (DR services unit.)
- Desmond Low (Product Manager), Singapore Telecom, EXPAN

Analysis and Discussion

The data collected from the NLB case study interviews and documents were developed into a (separate) formal case study. The contents of the case study and in-depth interviews with experts are documented and analyzed below on the basis of the research model.

DR Planning Process

NLB's DR planning practice and the views of the experts on this issue are summarized in Table 1. The general consensus, as reflected in the table, is that DRP needs to be a robust and comprehensive process and cover the following phases:

- Initiation of project
- Business impact analysis (BIA) and risk analysis (RA)
- DR strategy/plan development
- Implementation and test plan
- Maintaining the plan

Table 1: Data on DRP Process

Source	Views/Practices
NLB Case Study	○ **No official BIA** ○ DRP **carried out in phases for each system** ○ Seek top management approval after planning
Opinions of Experts:	
Dr. Goh Moh Heng (DRI Asia)	○ Lack of project planning and project initiation ○ **Lack of BIA** /applications analysis ○ **Responsibility fell on IT** ○ **Management** must **know the impact**
Mr. Wong Tew Kiat (Singapore Computer Systems Ltd)	○ BIA and RA implemented in the planning process ○ Complacent companies leading to **lack of BIA** ○ **No full-time DRP officer** in place ○ Common mindset: DR is **IT's job** ○ Need **buy in from senior management**

Ms Annie Phang (Singapore Computer Society)	○ Phases include:
	  ○ Form team and conduct gap analysis
	  ○ Understand business, mission, and major source of income and sales turnover
	  ○ Conduct BIA and RA for organizations
	  ▪ **Lack of BIA**
	  ○ Seek endorsement from management.
	  ○ Implementation and testing

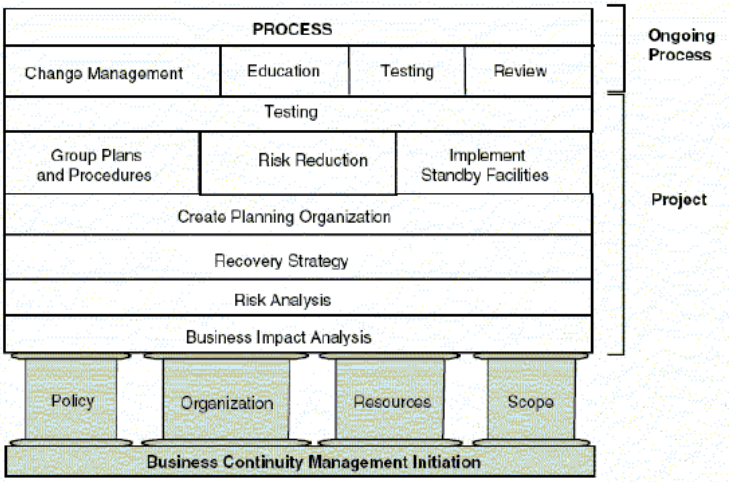


Figure 2: Gartner's Business Continuity and Disaster Recovery Model

Toigo's (2003) SDLC-type recommendations for DR planning and Gartner's (2004) Business Continuity Model (see Figure 2) synchronize with the consensus reflected above on DRP.

DRP Project Initiation

The DRP project was initiated in NLB by Kuan Sung, Senior Manager of Operations, who had decided that it was time to have a more comprehensive DR plan for NLB. Mr. Kuan had noted the growing reliance of the library on IT for delivery of a range of services including e-magazines and online databases. A team was formed, consisting of various system owners from NLB and staff from National Computer Systems. the vendor responsible for the systems.

The need for someone to champion a DRP initiative is clear from the NLB case study. Otherwise, such a need not may be apparent until too late; Beath (1991) has highlighted the virtues of a champion for success in an IT initiative, and DRP, in particular, would need such a champion. The champion would initiate the formation of the project team and DR steering committee to oversee DRP implementation. The team should consist of representatives from affected business functions and executive management to help garner organizational and management support for the DR plan.

Business Impact Analysis and Risk Analysis

Conducting business impact analysis (BIA) and risk analysis helps to set the direction and scope of the DR plan for an organization. However, many firms in Singapore, as noted by the experts interviewed, plunge into DRP without proper analysis of the threats faced and their impact on business. This was also noted in the case of NLB where no formal BIA had been conducted, resulting in the DRP project team not realizing the impact of a disaster to their systems and appearing to be not adequately prepared.

Without BIA and risk analysis, organizations would not be able to clearly identify the critical areas and potential threats faced and decide on what should be done for DRP. Such analysis would help in quantifying the organizational commitment, resources and arrangements required to mitigate the risks posed by disaster. An organization whose IT portfolio is largely in the "factory" and "strategic" quadrants of McFarlan's (1984) strategic grid (for analyzing the impact of IT on strategy and business operations) would certainly require far greater DR arrangements as compared to one occupying the "support" and "turnaround" quadrants. Critical and essential systems in the "factory" quadrant would require even far greater DR

arrangements as compared to pure strategic systems in the "turnaround" quadrant. Systems which are inherently of greater risks would require greater contingency plans which should include substantial DRP if these systems are essential or critical to the business.

The experts interviewed concurred that BIA and risk analysis should be done and the results should be presented to top management to clarify the potential dangers arising from inadequate DRP for IT. It would enable them to obtain the necessary financial support and resources for this critical organizational requirement. It would also provide a strong basis to tackle any lack of commitment from DR project team members who might view their roles in the committee as secondary to their core responsibilities. As noted by Gido and Clements (2003), lack of commitment is a common barrier to an IT project team's effectiveness and needs to be effectively addressed for project success – the value of BIA and risk analysis goes beyond planning to successful project execution. BIA and risk analysis would also help to highlight the need for the DRP team (consisting of senior IT professional and executives) to communicate with key IT-users on business requirements and critical systems and data. The experts interviewed noted that while DR responsibilities are handled by the IT department, the IT people responsible often fail to engage and communicate with IT-users on this matter, leading to lack of support and understanding from them.

Types of Disasters

Figure 3 models the types of disasters identified in the field work (see Table 2). The model developed in this study closely corresponds to that of the National Institute of Standards and Technology which categorizes disasters into natural, human and environmental [NIST, 2002].

Table 2: Data on Types of Disasters

Source	Views/Practices
NLB Case Study	○ Disasters identified: Fire, flood, power failure, hardware and software failure, web-based threats i.e. hackers and viruses, and customers' intentional or deliberate misuse of machines
Opinions of Experts:	
Dr. Goh	○ Possible disasters within Singapore: power failure, flood and explosion ○ Other disasters outside Singapore: **natural disasters** such as tornadoes, earthquakes, and the recent tsunami ○ Terrorism has become a major concern, particularly for the U.S.
Mr. Wong	○ Disasters are dependent on location e.g. Japan is in an earthquake zone ○ **Terrorism** is also a major threat for many countries
Ms Phang	○ **Natural disaster** e.g. fire, floods and tsunamis ○ **Man-made disaster** e.g. acts of terrorism and arson ○ IT disaster e.g. network failure

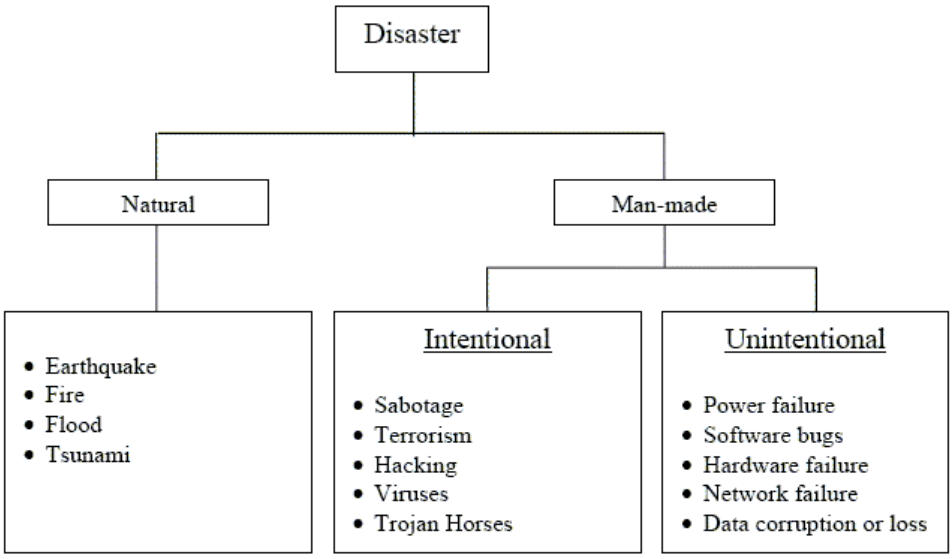


Figure 3: Model of Types of Disasters

Although natural disasters tend to occur less frequently, they are potentially more devastating. Hence, careful analysis is required to ascertain the potential dangers and make the required DRP arrangements. This is evident in the case of NLB which had catered for most of the disasters depicted in the model above with the exception of some uncommon natural disasters - Singapore is perceived to be less prone to natural disasters such as earthquake and volcanoes, hence this exception. NLB has rightly placed greater emphasis on intentional disasters due to the high usage of IT in its operations and exposure to users and others.

Business Needs of DRP

As noted in Table 3, IT is very important and strategic but not (yet) fully mission critical for the library. The library's operations and activities have been transformed by IT [Hallowell et al., 2001], but IT is not really critical for the library. The library has yet to reach a stage where a major failure in IT could translate into disaster for the organization as would happen to a bank or a stock exchange. As IT is playing both support and strategic roles in NLB, the library has not implemented a full-fledged comprehensive DR plan as a bank would. Perhaps, it was for this reason that a formal BIA was not even performed in NLB.

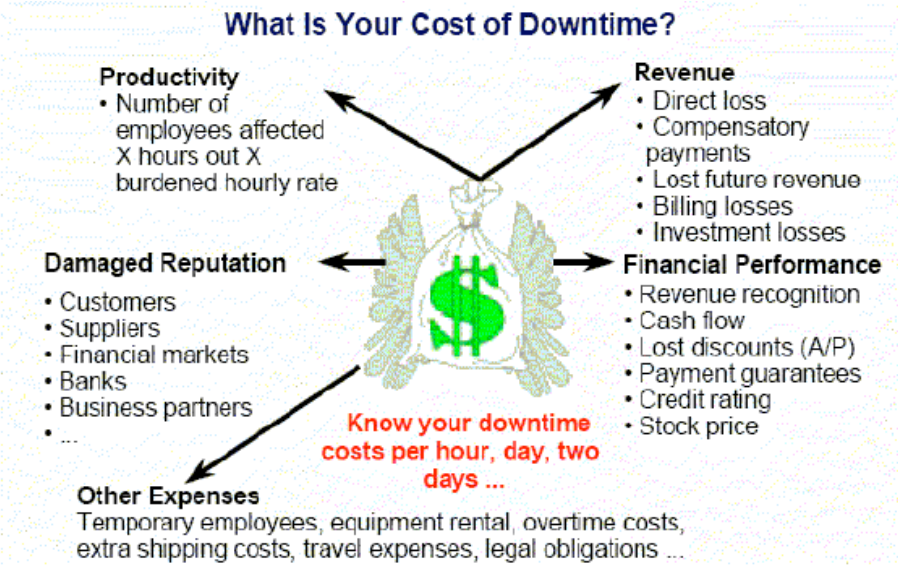
The consensus of the experts interviewed is that most organizations, in general, do not accord the necessary level of attention that DRP deserves (see Table 3). Only organizations such as banks and stock exchanges that are bound by legislation have sound DRP [Weiner, 2001]. It is usually difficult to convince an organization's management on the necessity for DRP - there would be no real ROI for the money spent on DRP. Efforts should therefore be made to quantify, via BIA or similar risk analysis, the potential losses resulting from a disaster to highlight the seriousness of inadequate investment in DRP. Y2K and 9/11 served as wake up calls for many organizations, but complacency tends to set in as time passes without any major disaster or incident affecting the operations of the organization's systems.

Although it is best for organizations to plan and prepare against all types of disasters, the resources required and the financial constraints have to be factored in when planning the required DR arrangement. Figure 4 shows Gartner's model for assessing the cost of disruption to business. By using the model and performing BIA, organizations are able to recognize their

critical business functions and the cost of downtime if a disruption occurs. By understanding the mission critical aspects of its business, an organization is able to implement sufficient DR

Table 3: Data on Business Needs of DRP

Source	Views/Practices
NLB Case Study	○ NLB functions not **mission-critical** enough to justify the cost of a full-fledged DR plan
Opinions of Experts:	
Dr. Goh	○ **BIA** identifies **mission criticality** ○ Losses classified as quantifiable or non-quantifiable ○ Legislation required banks to practise DRP ○ Industries with **high reliance on IT** should focus on DRP for the IT systems
Mr. Wong	○ **Difficult to convince management** of the need for BCP/DRP
Ms Phang	○ Many companies have **not done enough** (in BCP/DR) ○ Financial institutions need to have a robust DRP
Mr. Hii and Mr. Low	○ Local firms **do not have DRP** ○ BIA determines how critical business functions are ○ Zero **Recovery Time Objective (RTO)** requires huge investment in DRP



Source: "Preparing for a Disaster: Affordable SMB Actions", D. Scott, J. Browning, Gartner Research, 2002

Figure 4: Model of What is at Stake if a Disruption Occurs

measures to ensure continuance of the business in the event of a disaster to the systems enabling the business. Through proper analysis and assessment, organizations can avoid both

under- as well as over- investing in DRP. In this regard, an application portfolio-based approach is proposed later in the paper.

IT Applications

The most critical system in NLB was Vista, the library automation system which handled all aspects of operations from catalogues and enquiries to issuing and receiving of books and other materials. As this system was critical for the smooth functioning of the library, a comprehensive DR plan was developed and implemented specifically for this system. The DR arrangement covered live back-up of the databases and full back-up of application software as well as procedures and controls for the system on a "hot" site away from NLBs central data center at one of its remote libraries. This "hot" site was fully networked and ready to "kick in" should there be a major problem at the main data center. As a next step in the DR arrangement for Vista, NLB was exploring the possibility of engaging a third party to provide the required DR support. This would allow the library to take full advantage of professional support and competences to realize the necessary DR requirement at an economic rate.

While Vista was fully supported by a DR plan, the other systems in NLB had standard contingency arrangements, primarily in the form of back-ups of relevant databases and application software. Kuan, the senior operations manager, clarified that it would not be economically feasible to have full DR arrangements for all the systems. The DR arrangement would have to match the criticality of the system. Otherwise, it could amount to expenditure and effort not matching the requirement. The cost of downtime is one way to ascertain the extent of DRP required for a system.

Financial impact of system failure		
Application	**Industry**	**Hourly cost**
Brokerage operations	Finance	$6.45 million
Credit card sales authorizations	Finance	$2.6 million
Pay-per-view	Media	$150,000
Home shopping (TV)	Retail	$113,000
Catalog sales	Retail	$90,000
Airline reservations	Transportation	$89,500
Tele-ticket sales	Media	$69,000
Package shipping	Transportation	$28,000
ATM fees	Finance	$14,500

Source: "Application Note, Disaster Recovery and Business Continuation: Planning for Success", StorageTek, 2004

Figure 5: Typical Hourly Cost of IT Application Outage by Industry

Figure 5 shows that the financial impacts of disruption vary for different applications. It is therefore logical to develop DR plans for systems according to their relative significance/importance defined by the cost of outage. Systems that require zero recovery time or incur very high hourly outage costs would therefore warrant comprehensive DR arrangements and be given top priority. Mission critical systems need even more extensive DR arrangements as failure without appropriate DRP could mean disaster for the organization.

IT Infrastructure

IT infrastructure comprises hardware, operating system, other system software and networks based on a client-server architecture. From a DRP perspective, the most critical component of the infrastructure is the server. For NLB, a key criterion for the backup site for its (Vista) server was the availability of large bandwidth to handle the switch from the main data center with minimum interruption. A duplicate server was therefore set up at the backup site to enable a smooth recovery process. The NLB case study suggests that factors such as the availability of resources and facilities (networking, people, etc.) have to be taken into account for choosing the DR site and deciding on the arrangements.

Disaster Recovery Strategies

DR strategies can be classified as preventative or recovery [NIST, 2002]. Preventative measures include IT security measures, infrastructure redundancy and fault tolerance arrangements. They also include proper setup of the data center to cover operational requirements such as voltage stability and controlled temperatures. Recovery strategies are used when something happens to render the primary site inoperable; e.g., setting up an alternate site ("hot", "warm" or "cold" - depending on organizational requirements).

Table 4 documents a number of suggestions and strategies for DR identified in the field work. The chosen DR strategy should depend on the results of BIA and risk analysis of the organization's business and IT portfolio - a shorter RTO would therefore require more costly solutions like full duplex "hot" set-up. The level of DRP may also need to conform to any prevailing regulatory requirements relevant to the business, especially in the finance industry.

The specific DR strategy would depend on requirements as dictated by business needs, costs, extent of exposure to disaster, type of disaster and DR opportunities within the organization and the market. The following broad choices are available for DR – on-site mirror arrangement, remote arrangement within organization, mutual DR arrangement with another organization, third party commercial DR site, and off-shore DR arrangement. In the case of NLB, the strategy was a remote "warm" DR site within the organization.

DRP Challenges

The data from the DR experts and the NLB case study suggest that DRP challenges can be classified as business, technical and environmental. Business challenges may arise from attitudes and mindsets. Technical challenges may come about because of characteristics of the system and its implementation. Environmental challenges come in the form of new threats that organizations have to face, and this is certainly one area that needs full attention in the light of global terrorism and cyber threats such as hackers, viruses and worms.

The major challenge lies in convincing management of the necessity of DRP, especially when it requires substantial investments and high levels of commitment. Management is generally aware of the need for business continuity planning (BCP) but often fail to realize that DRP for IT is a critical component of BCP in today's business world. The key to gaining management support is through proper communication on the basis of sound analysis, arguments and case examples such as "Merill Lynch and 9/11".

Framework for Disaster Recovery Planning

This paper has researched and clarified some key issues on DRP for practice. The recommendations are not unique but are largely similar to that prescribed in standard DR references such as that from Gartner. The unique contribution of this paper is an application portfolio-based framework for macro level DR planning.

Table 4: Data on Disaster Recovery Strategies

Source	Views/Practices
NLB Case Study	○ **Measures in place**: ○ IT security measures ○ Fault tolerance ○ Redundancy of hardware, firewalls and network arrangements ○ Load balancing and clustering ○ Backup power ○ Backup practices such as disk imaging ○ DR project to set up **alternate site**: ○ Implementing disaster recovery site in phases ○ Working towards a complete, tested DR plan
Opinions of Experts:	
Dr. Goh	○ Strategies include backup and mirroring ○ Offsite tape backup (least expensive solution) selected when **budget** is low ○ Requirements determine strategies employed, with shorter RTOs warranting more costly solutions ○ **Mirroring** can be used with a **shorter RTO**, **tape backup** when **RTO** is **longer**
Ms Phang	○ **Backup** procedures have traditionally been in place ○ Banks outsourced for data storage solution ○ Project to **close gaps** identified previously ○ Good, robust **testing** plan to identify areas for improvement ○ Internal and external **auditing** ○ External auditors to help educate internal auditors on what to look out for
Mr. Hii and Mr. Low	○ Possible options: ○ **RTO** of **zero**: **dedicated room** and **mirroring** ○ **Less costly** solution: **shared workspace**

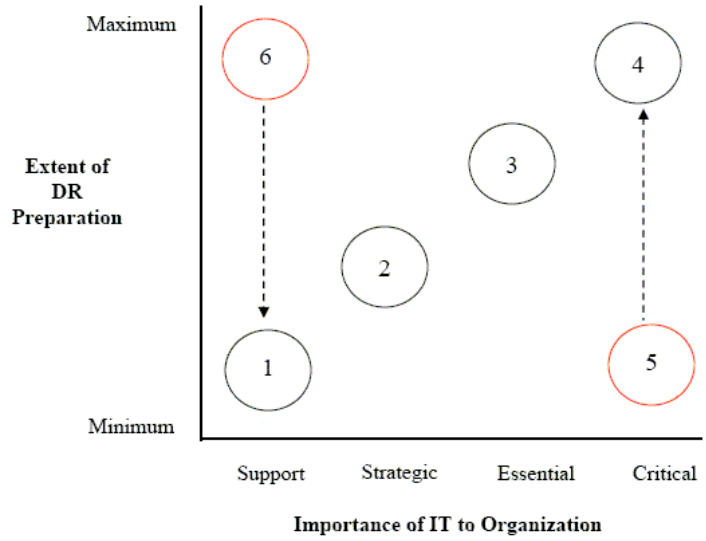


Figure 6: Macro-Level Framework for Disaster Recovery Planning

MacFarlan's (1984) strategic grid concept is a popular technique to assess the impact of IT on an organization's business strategy and operations. A practical way to assess the overall impact is on the basis of the organization's IT applications and their individual and collective impacts. This paper leverages on MacFarlan's strategic grid to propose the DR planning model shown in Figure 6 on the basis of the research findings. The vertical dimension reflects the extent of DR arrangements required for an IT application. The horizontal dimension reflects the major role played by that IT application in the organization:

- Support: The IT application is used to support functions like administration, office automation or create a web presence. If the application is down or destroyed, the organization can still fall back on paper documents and manual processes. The disaster will not cause the business to fold up but would affect its performance.
- Strategic: Breakdown or destruction of the IT application will impact the organization's competitiveness. The breakdown or destruction of the application will not disrupt business, but it would affect the organization's competitiveness. Examples are customer relationship management, supply chain management and e-commerce websites of click-and-mortar organizations. The sooner the application is restored, the sooner the organization can resume realizing strategic value from the application. Delay could have serious strategic consequences.
- Essential: After some time some "support" applications (e.g., accounting and financial applications) become an essential resource for an organization. Similarly, some "strategic" applications (e.g., ATMs for banks) become industry norms (i.e., essential to be viable in the industry) when others in the industry also implement similar applications to mitigate any competitive disadvantage. When an "essential" application breakdowns or is destroyed, the organization's operations would be immediately affected. It would be very difficult for the organization to continue until the application is restored. It may be possible for the organization to operate minimally without the application, but undue delay in the restoration of the application could have grave consequences for the organization's viability.
- Critical: Some "essential" applications become "critical" for the business. They are part of the critical resources for conducting business, and any failure or collapse would immediately translate into serious problems, if not disaster, for the organization. Without the application, there is no business (as in the case of stock exchanges) or even no organization (as in the case of dot.coms such as Google and Amazon.com).

An organization's IT application portfolio can be mapped on the framework shown above on the basis of the role of each application and the level of DR arrangement in place for it. As depicted, the DR arrangements for applications at nodes 1, 2, 3 and 4 are properly matched with the role and value of the applications to the business. On the other hand, the application at node 5 represents the extreme end of under-investment in disaster recovery planning. The organization is in a potentially disastrous position - the DR arrangements should be progressed upwards towards node 4 as soon as possible. Node 6 represents the other extreme end of over-investment in DRP. The organization can afford to cut back on the level of DR arrangements for the application and move it downwards to node 1.

Conclusion

As IT becomes increasingly fused with business, DRP also needs to keep pace. This paper has clarified the importance of DRP and has described practices for DR planning on the basis of research. An application portfolio-based framework for macro-level DRP has been proposed

for determining the required extent of DR arrangements for specific applications in an organization – the basic argument is that, for economic and pragmatic reasons, DR arrangements must be on application basis rather than on a total IT basis. Other researchers could explore the framework and other DRP models, thereby shedding more light on disaster recovery planning, an important IT management topic which is still lacking adequate research.

Many organizations do not have adequate DR arrangements. In Singapore, this is mainly due to the mindset that the country is safe from natural and other disasters. However, this perception is being challenged by the emergence of global terrorism, natural disasters and the proliferation of computer viruses, hackers and other threats. The 2004 tsunami serves as a warning to organizations, particularly in naturally safe countries such as Singapore and Malaysia, not to be complacent about DRP. Organizations should realize the risk and invest in DRP to safeguard critical data and application software. Proper DRP can minimize losses or even guarantee survival in the event of a disaster. Without DRP, successful businesses such as Merrill Lynch would have perished with the thousands of people in the September 11, 2001 terrorist attack of the World Trade Center in New York. Organizations should learn from them. The National Library Board of Singapore, despite IT not being a critical resource (as yet), has certainly recognized this and has started on the long but important process of disaster recovery planning.

References

ABA, "Thinking the Unthinkable". *ABA Banking Journal*, January 2002, pp.44.

Alonso, F., Boucher, J., and Colson, R.H. "Business Continuity Plans for Disaster Response", *CPA Journal,* 2001: 71(11), pp.60.

Ballman, J. "Merrill Lynch Resumes Business Critical Functions Within Minutes of Attack", *Disaster Recovery Journal*, Summer 2001, Vol 14, Issue 4

Beath, C., "Supporting the Information Technology Champion." *MIS Quarterly*, 1991: 15(3).

Brunetto, G., and Harris, N.L., "Disaster Recovery". *Strategic Finance*, March 2001, 82(9)

Cerullo, V., and Cerullo, M. J., "Business Continuity Planning: A Comprehensive Approach", *The Information Management Journal,* 2004: 21(3)

Gartner Research publications:

Claunch, C., "Management Update: Best Practices in Business Continuity and Disaster Recovery". *Gartner Research*, 17 March 2004:

Krischer, J. et al., "Six Myths About Business Continuity Management and Disaster Recovery." *Gartner Research*, March 2005.

Mingay, S., "Management Update: Many Challenges Faced by Business Continuity Managers in 2004". *Gartner Research*, 7th Jan 2004:

Scott, D., "Survey Confirms There Are Many Effective Disaster Recovery Strategies." *Gartner Research*, April 2005

Scott, D., and Browning, J., "Preparing for a Disaster: Affordable SMB Actions". *Gartner Research*, 6th March 2002:

Cougias, D., Heiberger, E.L., and Koop, K., *The Backup Book : Disaster Recovery from Desktop to Data Center*, Schaser-Vartan Books ,2003

Gido, J. and J. P. Clements, *Successful Project Management*, Thomson South-Western, 2003.

Hallowell, Roger, Knoop, Carin-Isabel, and Neo, Boon Siong, "Transforming Singapore's Public Libraries", *Havard Business Review*, 31 October 2001:

Hood, Sarah B., "Always Be Prepared." *Canadian Business*, March 2005: 78(6).

Maiwald, Eric, and Sieglein, William, *Security Planning and Disaster Recovery*, Mcgraw-Hill Book Co., 2002

McFarlan, FW, “Information Technology Changes The Way You Compete”, *Harvard Business Review*, May-June, 1984, Vol 62, No 3, pp93-108

McCarthy, "The Best Laid Plans", *Journal of Accountancy*, May 2004: 197(5)

Morganti, Michael, "A Business Continuity Plan Keeps You In Business", *Professional Safety*, Jan 2002: 47(1)

NIST,. *Contingency Planning Guide for Information Technology Systems*, National Institute of Standards and Technology, US Department of Commerce, June 2002

Nosworthy, Julie D., "A Practical Risk Analysis Approach: Managing BCM Risk". *Computers & Security,* 2000: 19(7)

Toigo, J.W., *Disaster recovery planning: preparing for the unthinkable*, Prentice Hall, 2003

Weiner, Stanley, "Managing Effective Disaster Recovery". *CPA Journal,* 2001: 71(12), pp.22.