Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 9 (2013) 795 – 805

Procedia Technology

CENTERIS 2013 - Conference on ENTERprise Information Systems / PRojMAN 2013 - International Conference on Project MANagement / HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies

Disaster Recovery – a project planning case study in Portugal

Antero Prazeres, Eurico Lopes *

Escola Superior de Tecnologia, Instituto Politécnico de Castelo Branco, Av. Empresário, Campus da Talagueira 6000-767 Castelo Branco, Portugal

Abstract

Business disruptions can take place everywhere, anytime. It is impossible to foresee what may hit and when. It has become compulsory for organizations to be organized for such disaster/recovery scenarios. With the ever increasing dependence on business processes for both electronic and traditional services, it has become almost mandatory for every organization to plan also for Business Continuity (BCP).

In this paper, a project plan to deal with a Disaster Recovery and support Business continuity and how various virtualization technologies are leveraged to reorganize restore servers, network and storage resources for the critical applications based on business priorities will be described. A project planning will be discussed in order to deal with a practical solution implementation in a major Portuguese organization

Keywords: Disaster Recovery (DR); Business Continuity Plans (BCP); Virtualization Technologies (VT)

1. Introduction

Disaster Recovery Planning (DRP) [1, 2] is associated with the recovery of a key set of IT systems and infrastructure components. The Business Continuity Planning [2, 3, 4, 5] is related with the enterprise as an whole piece dealing with business processes. So, Disaster Recovery (DR) thoughts are part of the Business

* Corresponding author. Tel.: +351-272-339-334; fax: +351-272-339-399.
E-mail address: eurico@ipcb.pt.

doi:10.1016/j.protcy.2013.12.088

Continuity (BC) [4, 5]. Business Continuity involves more than recovering an organization's IT environment in the event of a disaster [5]. Business Continuity insures that an organization can restore its IT systems and business processes – attainment workforce back to work, serving customers, collecting revenue, and continue operations [6]. In this paper it is intended to evaluate which applications are critical services of organization to justify their relocation to an alternate site to ensure the availability of these applications in the event of partial failure or general production systems on the main site and then develop an implementation solution guided a Project Management Institute (PMI) project.

So, this paper discusses a project planning proposal to implement a Disaster Recovery & Business Continuation solution in large organization in Portugal, using the latest technologies from VCloud and vSphere as virtualization technologies [3, 7].

2. Theoretical Perspective

From the IT perspective recovery will usually stand for establishing support for the processing and communications functions considered crucial by the business society and then establishing support for subsidiary systems. From the business perspective recovery will mean, being able to execute the business functions that are at the centre of the business and then being able to execute subsidiary functions. It is essential that issues that may affect Business Continuity be documented and addressed as part of the DR endeavour, even if the only action taken is to postpone them to the BCP team, or to bring together them as input to a future BCP effort if this is a separate DR project [4, 5].

Timeframe is another key issue to consider when defining recovery. Is the goal to have all systems up and running within an hour, a day or a week? Is it enough to only discuss a few key systems within the first week, while taking longer to restore others? This factor is often expressed as either the "Recovery Time Objective" (RTO) or the "Service Delivery Objective" (SDO). This refers to the amount of time that can pass by from the failure to the time when the systems or services are available for use [8, 9].

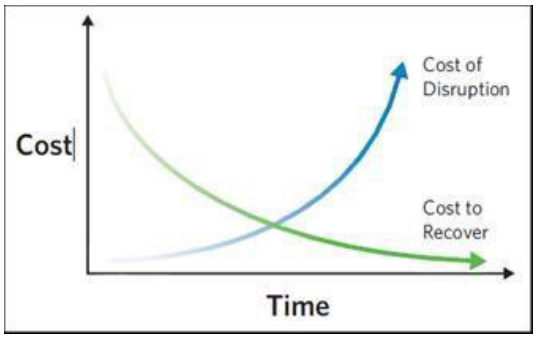

Fig. 1. Relation costs of disruption/recover

The Recovery Point Objective (RPO) expresses the data we may afford to lose. Depending on the infrastructure the loss of any data possibly will have a major impact. The lower the RPO, the higher the overall cost of maintaining the infrastructure environment for recovery [8,9,10].

3. Related Work

Latterly, many research works encompass in the crisis management and disaster recovery support theory [11]. However, most of these have purposeful on time critical information sharing among emergency services such as hospitals units. Others have focused on information sharing and collaboration along with administration agencies.

Another study endeavour presents time critical services implemented for the Emergency Management Services in Canada [11, 12]. The structure involves teamwork along with public/private entities such as the emergency phone system, Police Department, Fire Department and Hospitals. The authors indicate that the implementation of such a framework assisted in getting better the general response time and performance across diverse organizations [11]. The framework uses several modes of information switch over and communication such as radios, telephones and interfaces for patient data sharing.

Agarwal et. al., stress upon the impact of Geographic Information Systems for disaster recovery [13]. The system offered in their research work uses failure related information from Emergency Operations Centers at local, state and federal level. However, the above systems lacked collaboration amongst businesses and emergency supervision officials necessary for efficient disaster preparation and convalescence efforts.

The model offered in this paper attempts to deal with all the weaknesses of the abovementioned research efforts and uses upon their strengths facilitating the design and development of a Business Continuity for rapid disaster recovery, sustained by a provider cloud infrastructure.

4. Research Methodology

To frame the main research design the following research questions aim to be answered:

- Should be possible to integrate organization legacy systems into a common infrastructure that will be able to work as one in case of failure?
- What shall be the requirements, the problems to tackle, critical business processes, licences needed and system maintenance?
- How to support business continuity in case of failure?
- How to maintain the system running in order to support decision-making and reporting?

The research methodology used was action-research [25, 26] and it involves the process of actively participating in an organization change situation whilst conducting research. This was done by the researcher while be a member of team as part of a community of practice, as it is the whole organization. Action research can also be undertaken by larger organizations or institutions, assisted or guided by researchers, with the aim of improving their strategies, practices and knowledge of the environments within which they practice. This was also done, when dealing with technological issues in order to design and discuss an implementation solution.

5. Critical Points

Revising organization business processes we identified the following critical points:

- Need to consolidate data storage;
- Identification of applications considered critical and requiring continued business;
- Identification of possible sites and feasibility studies of the same;
- Identification of all internal project stakeholders;

- Establishment of milestones of the project, being conditioned by the decision to acquire higher material and bids for the same;
- Identification of technologies intended / required;
- Identification of necessary infrastructure for the datacenter new installation of racks, as well as the needs of infrastructure networks needed for communication and data replication inter-sites.

Thus the development of a project in the organization will allow the evaluation of infrastructure present and identification of their critical applications, evaluate and organize existing backup systems and storage, and find the ideal compromise between the recovery time (RTO) and service delivery (SDO). Considering the areas of business and information involved in the organization, so faster services are available and the lower the risk of data loss better. Virtualization plays an important role nowadays due to its versatility and modularity, allowing keeping costs at acceptable levels. The aim is to increase the level and optimizer virtualization, in order to obtain the best value for RTO / SDO possible and at the lowest cost possible.

6. Organization Infrastructure

The main structure of the organization may be divided into two parts: (1) Game and (2) General Services. The Game component in not part of the main study since it as considered an external business, but still has some influence in decision making and physical needs.

Thus, in general, the infrastructure consists of HP-UX, Windows and Linux systems all connected to a HP EVA 5000 SAN. The HP EVA is discontinued and there is no plan for maintenance. In terms of scalability and modularity it is at his limit, and does not allow any kind of physical and upgrade systems and it does not support the latest technologies of virtualization.

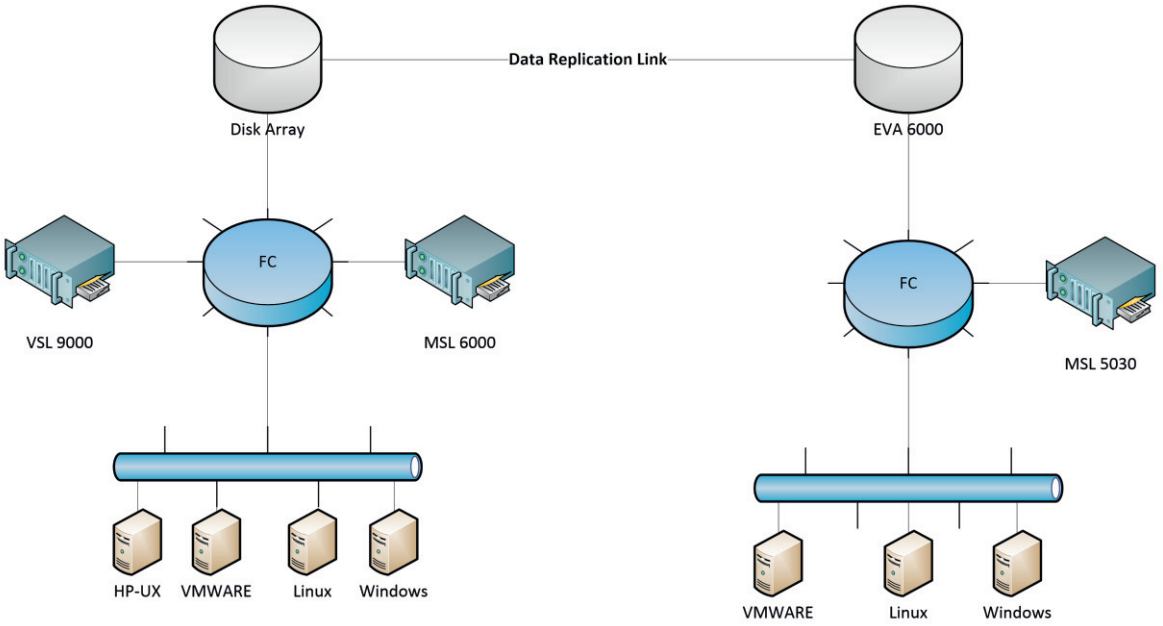

Fig. 2. Main site and Recover Site

The infrastructure of the organization consists on Windows and Linux systems, fully x86, existing in a Private Cloud based on VMWare technology and physical systems from HP DL 360 and DL 380, interconnected in a HP EVA 6000 SAN.

The entire network based on Fibre Channel links and routers CISCO / HP is the external link provided by Portugal Telecom (PT).

The existing databases are Oracle and Microsoft SQL, and existing applications to create highly heterogeneous inside the house or outside vendors. All business logic is based on SAP systems.

The primary activities of the business and social action are: management of the network of homes for the elderly / children / disadvantaged, hospitals that exist in the Lisbon area, maintenance of assets of the same, apart from the Game.

At present there are four datacenters in organization's infrastructure, present in the same building, and one more in a Disaster Recovery on the premises of PT in Picoas, Lisbon, as well as two storage systems in datacenters present in the main building and one in the PT. For this, there is the desire and need to standardize the storage systems so that there is only one storage environment in the main data centre and one more in a disaster recovery.

This solution is already at its limit of expansion due to limitations of the physical infrastructure of servers. Yet it is enough to receive Disaster Recovery intended.

The intended architecture is based on a virtualization solution with VMware server pool at both sites and is based on hardware-level replication of storage between the two sites. Figure 2 shows the basic system architecture considered. It consists of a primary and a backup site. The primary site will be composed by a new SAN with virtualization capability, two backup systems (disks and tapes), an infrastructure x86 based, all connected by fibre channel. It will be the "primary" part of the private cloud of the organization. The backup site will have the actual EVA 6000 or the existing EVA 4000 upgraded with 6000 parts interconnected with x86 infrastructure and a tape backup platform. This will be the "secondary" part of the cloud.

The backup stores enough information so that if the primary fails, the information stored at the backup may be used to recover data lost at the primary. Furthermore, the backup may take over after a failure. Depending on how the backup site functions, we classify recoverable systems as data recovering or service recovering. A data recovering system only recovers or restores data to a consistent state when components of the system fail. The system may stop providing services until the components are repaired. With service recovering systems, data is recovered while systems provide continual services.

7. Technological Considerations

There a several technological possible solutions to deal with a disaster recovery and business continuity processes. Older solutions are based on backup systems which provide a later recover in a day time scale of re-operation. Others based on redundant systems based in same site – when a transition is accomplished it is also created a replica in a redundant system implement with that purpose. The main problem with this solutions, reside in the fact if catastrophe occurs in the plant site, the probability of both systems break down are very high. So, business continuity may not be possible in this case of calamity.

However, in the past decade, virtual networking started with a simple bridging of VM's virtual network adapter to host's physical network adapter in VMware's Workstation product [14]. With VMware's vSphere product, virtual networking has evolved to a distributed virtual networking infrastructure with pluggable packet switching and filtering modules, under the umbrella marketing name of vNetwork.

Also the emergence of the Cloud Computing paradigm [15, 16] enables cloud users to lease infrastructure resources from public clouds acting as Infrastructure as a Service (IaaS) utilities.

Public cloud providers like Amazon [17], Google [18], Microsoft [19], GoGrid [20], and IBM [21] offer cloud users the ability to deploy virtual applications composed of multiple VMs and easily scale them, without

making sizable capital investments in computing hardware. An important application for cloud providers is the ability to support a cloud raging scenario [1, 7]. Private clouds are limited in the amount of resources they can pre-allocate for spikes in claim. Cloud break open refers to private clouds offloading work to public clouds to handle a spike in demand [15]. This allows the private clouds to control their total cost of ownership since they do not have to invest in resources just to handle uncommon peaks in demand. To transparently upload the private cloud, live long-distance mobility is required between the private and public cloud. A second important application for long-distance inter-cloud mobility is enabling load consideration and high availability services between cloud providers. Similar to the way in which small ISPs rely on larger ISPs for their connectivity [24], a small IaaS provider may depend on a larger IaaS provider to secure the availability of services to its customers [14, 15].

Cloud computing is built on a self-service model, where consumers present a workload and all provisioning and exploitation is automated [14]. Currently, cloud providers present common grained service levels for consumers to choose from, which works fine for standard workloads. As cloud computing evolves, we would expect consumers to specify service requirements in a prescriptive way and the cloud infrastructure to dynamically prerequisite the necessary resources to meet the requirements. This presents the critical challenge to distributed virtual networking where all services are standardized and deployed on demand at per-VM granularity.

In general, different clouds normally include independent storage and network environments and are separated by firewalls. Any solution for inter-cloud mobility must maintain the insularity of the respective clouds in support of each cloud's IT infrastructure autonomy, privacy, and security requirements [22]. Migrating VMs across clouds therefore requires the following (1) enabling the move of memory and state between anonymous hosts, each residing in its own cloud; (2) ensuring that the VM will have access to the same storage at the destination host, without the two sites sharing storage; and (3) ensuring that the VM will have access to the same LAN at the destination host, without the two sites sharing the LAN. In this paper, we present an implementation of a technology that supports the above three requirements, thus enabling live mobility of virtual machines between clouds, while enforcing clouds' insularity requirements, using a public cloud provider, such as the case Portugal Telecom.

8. Planning Disaster Recovery

A Disaster Recovery project is a job which is never completed – project planning must be tested and revised several times during his lifetime. A project plan that does not afford place for changes in the organization it will be itself a disaster. Therefore the main objectives of a Disaster Recovery are to guide the business to successfully re-establish business operations within the shortest possible time with a minimal impact and loss of data. So, planning expected vulnerabilities and define the requirements of the business and IT infrastructure, design and them implement risk measures providing the organization with a disaster plan.

Disaster Recovery Planning must attend to the processing needs of the business society; this means key members of the business society must be concerned in the preparation to insure that these needs are adequately recognized [23, 24]. The following are some of the points which need to be addressed: Senior management must understand the effort needed and must commit to ensure its success; a project team must be selected that incorporates an adequate balance between IT and business community members; Solutions to fit the needs of the business and the IT communities and finally the final Plan needs to be incorporated with any other active plans such as Emergency Plans or Evacuation Plans, etc.

Given the presence of x86 systems only in the organization infrastructure, HP-UX system, it was decided to expand the current Private Cloud systems based on VMWare technology. This technology also allows for high availability across the infrastructure, it also allows a great modularity and scalability with lower costs the same. Through a connection Continuous Access between sites and between EVA's, VMWare allows you to have a

cloud shared between sites, being completely transparent to the client and the virtual machines where you are to perform data processing and which consumes resources.

So we intend to implement the latest technologies from VMWare under contract for existing Enterprise Plus. VCloud (Infrastructure as a Service (IaaS) framework and API), VMotion (move running virtual machines from one physical server to another with no impact to end users) and High Availability (), and the new version of vSphere (a complete, scalable and powerful virtualization platform, delivering the infrastructure and application services needed to transform their information technology and deliver IT as a service) are new virtualization technologies that are expected to reduce costs clearly. It also lets you take advantage of the DR site for development in order to optimize resources and justify the cost of the DR in addition to high availability [23, 24]. Other areas that will improve cost will be the processing and energy, because with the new version of vSphere also allows the machines used are not off saving the current session and user memory and when the machine is needed only takes a few seconds to be back online and in the initial state.

9. Planning Project Steps

Projects are characterized like every organization - unique, so each Disaster Recovery planning project is also unique. As such, what works for one business will not necessarily work for another. And a project is unique in that which is not a routine operation, but a specific set of operations designed to accomplish a singular goal. The following are the major phases and guidelines that we use as part of our DR Planning strategy, under the umbrella of Project Management Institute (PMI®); however these are guidelines only and may be modified as necessary by organization requirements.

- Project Initiation: gain an understanding of the existing and planned future IT environment of the SCML, define the scope of the project, develop the project schedule, and identify risks to the project. Additionally, a Project Sponsor/Champion and Steering Committee should be established during this phase;
- Risk Assessment - assessment of geographical location, computing environment, installed security devices, computing access control systems, personnel practices, operating practices, and backup practices;
- Impact Analysis - identify which systems and functions are essential to the continuation of business, and to determine the length of time that those units can survive without the critical systems in operation;
- Definition of Requirements - the plan must be detailed with the recovery requirements of the business and lT infrastructure, and the requirements generated by the assessment of risk;
- Project Planning – definition of the project that is being executed and to mitigate the disaster risk as possible;
- Project Execution - project should proceed according to standard practices of Project Management. During the project the Disaster Recovery Plan will be constructed and tested;
- Integration - integrate back into the organization's overall Business Continuity processes. For organization it is important to align the DR and BC;
- Maintenance - the ongoing maintenance and testing efforts required to keep the plan updated, as well as mitigate future risks as they are encountered.

This methodology, although it allows to define very well what is required and how to be studied, developed and implemented implies some limitations, particularly in terms of errors, the need to determine the prerequisites and it is assumed that once a phase is complete not turn the previous phases.

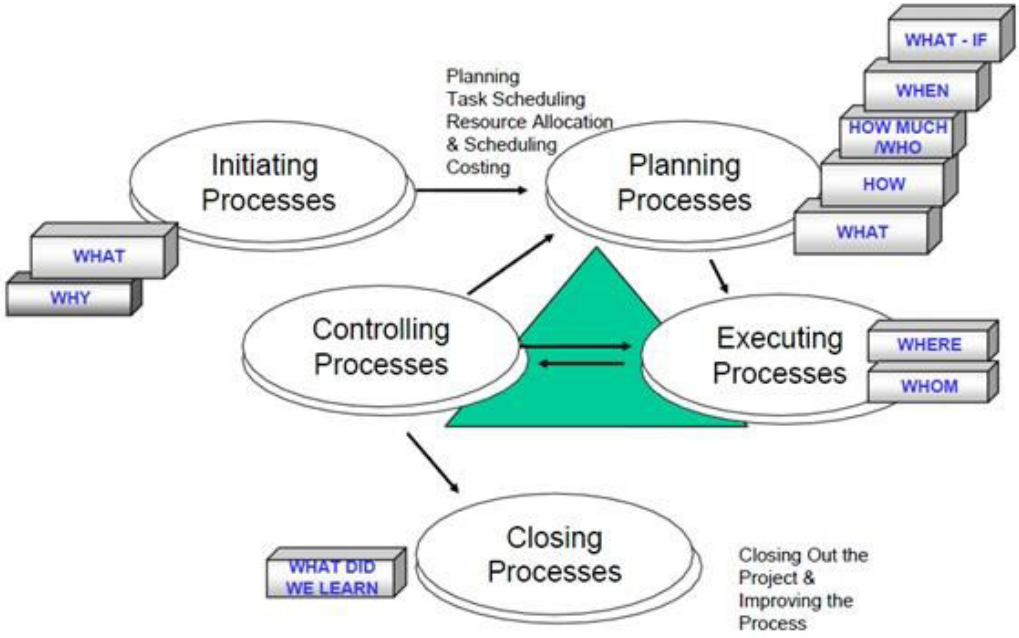

Fig. 3. Project Management Process (Paulo Gomes, 2010, 1.1.12)

Project management is to plan, schedule and control a set of project tasks to achieve project objectives on time, using an appropriate level of resources. As part of project management we have network analysis, work breakdown structure, planning and scheduling, control techniques, budgets, responsibility matrix, network diagram and Gantt charts, which are the technical elements of the project. Together with these elements have the motivation, training, counseling, team creation, conflict resolution, negotiation and communication as the most human part of the project.

Other problems with this methodology are it involves very high costs if changes are needed, the vertical integration of the system is applied in a very late stage of the project, undervaluation of sub-processes and integrations necessary and rejection if not exactly what you want. Another factor to consider is that over time the value that the project back to the company with Waterfall declines dramatically.

The methodology chosen for this project was the Agile, which although it is defined as being a bit rambunctious, will allow the project team to adapt over time to business needs and deliver prototypes and deliveries to increasingly approaching the final product. If we use iteration fixed and / or temporal fixed iterations have the advantage of focusing in terms of time and allow meet deadlines. The main difference is that this method works in increments, allowing back stage back and makes changes as necessary (figure 3). It also allows knowledge to be tapped to develop the next steps. The initial research and planning will reduce the uncertainty of objectives, allowing that there are buffers and contingencies that will help me prepare for the unexpected. The duration of the project is also reduced, acceptability of the end user is larger because of its greater surroundings reduces the risk of design and planning, construction and applicability thereof is more efficient.

This methodology is also known by different names: Concurrent Engineering, Fast Tracking and Agile Project Management. If it was a software project would Feature Driven Development, Rapid Application Development (RAD), Extreme Programming (XP) and Lean Development. If technically possible, there are

sufficient resources, the quality is not called into question and there care over time, one can reduce substantially the time of project leadership, enables better communication with management (top or not) and prevents iterations. This approach allowed for the necessary changes to the project due to several factors that have emerged, such as changing specifications scope, limitations of infrastructure and its adaptation-

10. Project Planning

The Project Manager has the overall authority and responsibility to manage and execute the project in accordance with its Project Plan and its subsidiary management plans. The project team will consist of teams of personnel Management Systems and Database and Network Administration.

The project scope of this project is the entire IT infrastructure. Was determined from an exhaustive analysis process requirement. It was initially identified the failure of the absence of a DR plan by the organization, for general services. We performed an analysis of the existing infrastructure in the company and identified which applications considered critical. Were thus identified business needs to ensure Disaster Recovery and especially business continuity in case of disaster.

The description of the project and its deliverables were developed based on the requirements gathering process, the analysis of the existing infrastructure and future needs of the same, risk analysis and external experts in communications, software and infrastructure. This help of external experts provided important data in order to analyze the current situation and what is sought, deciding which location to the site, which the best technical solutions in terms of physical infrastructure and virtual and optimize to the maximum existing solutions in order to keep costs in check and within budget.

After determining the scope, WBS, timelines and requirements is that management can accomplish this. After a careful analysis of what is required and how the tasks will be executed this project and based on the risk report, it is concluded that this project is low risk. In this project there are 6 possible risks areas: Delay in delivery of Material; Delay in infrastructure networks; Delay in supply Infrastructure; Scaling air-conditioning; Failed communications between servers; Communications failure between sites and Break of service.

11. Conclusions

We have presented a Disaster Recovery project model IT sharing among businesses for organization community under disaster/crisis situations. The model identifies the key components for disaster preparation, recovery and business continuity while stressing upon the need of better and improved tools and technologies for rapid recover. We then use our model for the implementation of Inter-Cloud VM based Business continuity, that creates a disaster management project plan based on the communication among the organization and that enables businesses and emergency management community: identify and assist in the execution of preparation and recovery plans; identify user relevant recovery resources along with the business/employee assistance programs facilitating decision support; and preparation of recovery infrastructure and related processes. General purpose cloud potentiates how IT services dynamically duplicated and later consumed in a Disaster/Recovery scenario.

The methodology used in this project will allow modularity and speed up the work, if properly implemented and coordinated. In terms of the project itself have the advantage of being almost linear, because there is no need to determine critical paths through techniques of CPM / PERT used by PMI. It is a fairly straightforward design and the material procurement and increased the primary determinant.

Completion of this project will enable the creation of DRP and will be used to sensitize the administration of the need of creating a BCP. In a future project and larger power will create a BCP for organization or adapt what is the game for the entire company.

In terms of IT this project will bring many benefits to the company as it will have a Disaster Recovery of the entire existing structure, update and optimize the virtual infrastructure, allowing it to be much more modular, consolidate information, reduce costs and enable business continuity.

We are currently developing the project. We need more research extending our network services to support virtual application access to the public network across clouds – mainly the requirements phase. This innovation will enable inter-cloud mobility of entire virtual applications assuring Business Continuity, the remaining project. Future work will also be focused in the Project Execution, Integration and Maintenance-

Acknowledgements

We acknowledged the Santa Casa da Misericórdia de Lisboa and we are in indebted to all those participants in this research - to them we present our gratitude.

References

[1] Jon William Toigo (2003): Disaster Recovery Planning: Preparing for the Unthinkable (3rd Edition): Harlow, UK: Prentice Hall.
[2] Susan Snedaker (2007): Business Continuity and Disaster Recovery Planning for IT Professionals, Syngress Publishing.
[3] R. Cegiela (2006): "Selecting Technology for Disaster Recovery." Proceeding of the International Conference on Dependability of Computer Systems, DEPCOS-RELCOMEX'06
[4] BCI Business Continuity Institute (2007): "Good Practice Guidelines 2007, A Management Guide to Implementing Global Good Practice in Business Continuity Management." Version 2007.3, October 2007.
[5] Kibildis, George W. (2005): Business continuity planning in the real world, Disaster Recovery Journal, vol.18 (3).
[6] Brett J. L. Landry and M. Scott Koger (2006): Dispelling 10 common disaster recovery myths: Lessons learned from Hurricane Katrina and other disasters. J. Educ. Resour. Comput. 6, 4, Article 6
[7] S. Maitra, M. Shanker, and P. K. Mudholkar (2011): Disaster recovery planning with virtualization technologies in banking industry. In Proceedings of the International Conference & Workshop on Emerging Trends in Technology (ICWET '11). ACM, New York, NY, USA, 298-299.
[8] Yoichiro Ueno, Noriharu Miyaho, and Shuichi Suzuki (2009): Disaster recovery mechanism using widely distributed networking and secure metadata handling technology. Proceedings of the 4th edition of the UPGRADE-CN workshop on Use of P2P, GRID and agents for the development of content networks (UPGRADE-CN '09). ACM, New York, NY, USA, 45-48.
[9] Nickolett, Chip (2001): Disaster Recovery Planning – Process & Options – A Framework for the Disaster Recovery Planner, White Paper, Comprehensive Consulting Solutions, Inc. see http://www.comp-soln.com/DRP2_whitepaper.pdf [Assessed 25/May/11].
[10] Manhoi Choy, Hong Va Leong, and Man Hon Wong (2000): Disaster recovery techniques for database systems. Commun. ACM 43, 11es, Article 6 (November 2000).
[11] Horan, T. A. and Schooley, B. L. (2007): Time-critical information services. Commun. ACM 50, 3 (Mar. 2007), 73-78.
[12] Schooley, B., Marich, M., and Horan, T. (2007): Devising an architecture for time-critical information services: interorganizational performance data components for emergency medical service (EMS). Proceedings of the 8th Annual international Conference on Digital Government Research: Bridging Disciplines & Domains (Philadelphia,Pennsylvania, May 20-23, 2007) 164-172.
[13] Agrawal, P., Rauschert, I., et. al. (2004): Multimodal interface platform for geographical information systems (GeoMIP) in crisis management. In Proceedings of the 6th international Conference on Multimodal interfaces (State College, PA, USA, October 13 - 15, 2004). ICMI'04. ACM, New York, NY, 339-340.
[14] Shudong Zhou (2010): Virtual networking. SIGOPS Oper. Syst. Rev. 44, 4 (December 2010), 80-85.
[15] Kenneth Nagin, David Hadas, Zvi Dubitzky, Alex Glikson, Irit Loy, Benny Rochwerger, and Liran Schour (2011): Inter-cloud mobility of virtual machines. Proceedings of the 4th Annual International Conference on Systems and Storage (SYSTOR '11). ACM, New York, NY, USA, Article 3 , 12 pages.
[16] M. Armbrust, A. Fox, R. Grith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia (2009): Above the Clouds: A Berkeley View of Cloud Computing. Technical Report UCB/EECS-2009-28, EECS, University of California at Berkeley, Feb 2009.
[17] Amazon. The Amazon Elastic Compute Cloud (EC2). See http://aws.amazon.com/ec2. [Assessed 7/Jun/11].
[18] Google. Google AppEngine. See http://code.google.com/appengine/. [Assessed 7/Jun/11].
[19] Microsoft. Windows Azure. See http://www.microsoft.com/windowsazure. [Assessed 12/Jul/11].
[20] GoGrid. Gogrid. See http://www.gogrid.com. [Assessed 17/May/11].
[21] IBM. IBM Cloud. See http://www.ibm.com/ibm/cloud/. [Assessed 5/May/11].
[22] Bernd Grobauer and Thomas Schreck (2010): Towards incident handling in the cloud: challenges and approaches. Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW '10). ACM, New York, NY, USA, 77-86.

[23] Manish Pokharel, Seulki Lee, and Jong Sou Park. (2010): Disaster Recovery for System Architecture Using Cloud Computing. Proceedings of the 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT '10). IEEE Computer Society, Washington, DC, USA, 304-307.
[24] Orran Krieger, Phil McGachey, and Arkady Kanevsky (2010): Enabling a marketplace of clouds: VMware's vCloud director. SIGOPS Oper. Syst. Rev. 44, 4 (December 2010), 103-114.
[25] Argyris, C. Putnam, R. & Smith, D. (1985). Action Science: Concepts, methods and skills for research and intervention. San Francisco: Jossey-Bass.
[26] Stringer, E.T. (1999). Action research. Thousand Oaks, CA: Sage Publications.