DISASTER RECOVERY AND BUSINESS CONTINUITY

PhD., Stefan IOVAN[1,2]
[3] *West University, Computer Science Department, Timisoara, ROMANIA*
[4] *Railway Informatics SA, Strategy Department, Bucharest, ROMANIA*
PhD. Candidate, Cristian IVANUS, *The Bucharest University of Economic Studies, ROMANIA*

ABSTRACT: Disaster Recovery (DR) and Business Continuity (BC) concepts began to have an increasingly audience in recent years in Romania. However, the level of expression of interest to the adoption and continuous efficiency of such solutions, the Disaster Recovery solutions authors and local integrators face a wide range of attitudes and expectations of the potential customers. Expressions of interest covers the whole spectrum of attitudes from stated passivism, argued with risks minimization (although in most cases it is about ignoring them) until addressing the so-called "*optical insurance policy*" concepts, giving up the proactive strategy that is essential for an effective business continuity plan. With the increasing technological capabilities that ensure business continuity, organizations have rapidly aligned to new standards and began to include mobile and cloud applications in the scope of disaster recovery plans.

KEY WORDS: disaster recovery, business continuity, cloud computing, disaster recovery planning, business continuity planning.

1. INTRODUCTION

Recent years rapid technological changes, and extreme climatic events faced by organizations around the world have reiterated the importance of business continuity management process. If only few years ago, the development and implementation of business continuity plans were seen by many as a necessary evil, an often legally but producing only additional costs requirement, at this moment organizations are recognizing the increasingly proactive role and importance of continuity management program [1, 2].

Business continuity is "*the work done by an organization to ensure that essential functions of a business are always available to customers, suppliers, business rules and other entities that must have access to these functions.*"

Other definitions are consistent with the definition of BS 25999-2:2007, the British Standard for business continuity management that states the business continuity as the "*strategic and tactical ability of an organization to plan and respond to incidents and business disruptions in order to continue business operations in a predefined level as acceptable*".

Definitions for disaster recovery are less clear inducing a certain level of confusion. Thus, according to the business dictionary, disaster recovery is the process of "*return of an organization, company or system to a state of normality, following a disastrous event*". The definition seems equivalent to the definition of business continuity. A similar but slightly more general definition: "*the process, policies and procedures related to preparing for recovery or maintain the health of the* *technical infrastructure that is critical to an organization after a natural disaster or man-made after an attack*".

Despite ambiguities in the above definitions we may conclude that disaster recovery is a technically oriented concept and is related to ensuring the operation of the technical infrastructure of an organization, while business continuity is a operational oriented concept related to and providing conditions for business performance. Therefore, disaster recovery is a component of business continuity.

Between business continuity and disaster recovery must exist a conditionality relation in the sense that disaster recovery plan must meet the requirements of business continuity. If this conditionality is not taken into consideration, financial resource consumption on various recovery solutions will be useless. A technical solution for disaster recovery, no matter how modern and ambitious it is, cannot guarantee the business continuity.

A global market study released at the end of 2011, with regard to the status of implementation of business continuity programs in organizations, highlighted the importance of this area. The objective of the study was to determine the maturity of the processes implemented by organizations around the world (including Romania) to ensure continuity of operations in case of necessity.

Study results have shown that business continuity processes not only remain on the agenda of management, but moreover, increased in importance and were aligned to the new challenges of the market, no matter whether they are related to new technology or in the change of how to do business (such as Cloud Computing or social networks).

60% of organizations that participated in the study have a well developed business continuity management program. The result is not satisfactory in the light of recent year’s events: devastating earthquakes in Japan, New Zealand and Italy, volcanic eruptions in Europe or extreme weather events in the United States. We believe that number should lie far above that, respectively a larger number of organizations should be prepared to respond as efficiently as possible if a major incident would affect its operations.

A key point in defining and implementing business continuity processes is to identify the reasons or business reasons that may lead to operational unavailability of any organization. From this perspective the study shown that organizations are more careful to the reputational impact than a few years ago.

Specifically, if six years ago only 14% of survey participants were writing that reputation is one of the reasons they decided to implement a business continuity program, now nearly 40% of them cited reputation as a key aspect key program implementation. Further, in line with previous years' results, ensure operational continuity, legal requirements or recommendations received from audits remain the main reasons for which organizations develop and implement business continuity programs.

This growth is not random. Exponential growth of the social media networks has and will continue to have a significant impact on the way organizations are doing business. Companies become more visible on these networks and therefore the information about these organizations run much faster.

More likely, an incident that could affect a company's ability to do business will be disclosed much faster than would have happened a few years ago and therefore, the reputation of an organization will be much faster and more affected.

1.1. Cloud computing and business continuity

A surprising result of the study shows that less than 40% of respondents do not know how much of the data the companies they represent are stored in the cloud, although a growing number of organizations are using or intend to move some information systems in the cloud. Without the correct and complete information about the location of data storage, companies are likely to fail in the early stages of implementing business continuity program. Organizations do not collect and therefore do not have relevant data concerning the impact of an unforeseen event could have on business and consequently, the size of the preparation effort for continuity is not appropriate. This often leads to significant investments in business continuity program that are not justified on business grounds [2 - 4].

Although moving systems to the cloud has its benefits (both operationally and in terms of reducing the risk of unavailability of systems), organizations are faced with an additional problem when it comes to the business continuity: Integration of own continuity plans with cloud solutions provider [5].

The study shows that the degree of integration has a downward trend, less than a third of study participants having a high degree of own integration plans with those of third parties dependants for running their business.

1.2. Mobile applications and business continuity

Another important aspect revealed in this study is related to the means on how organizations take into account the new market challenges, namely mobile applications and social networks. With a growing number of mobile applications and / or social network users, organizations are forced to change their way of thinking and doing business, and this is reflected in the preparations they make for contingencies [7].

The study shown that over 40% of participants stated that they use and have a recovery plan for mobile applications. Also, a growing proportion of organizations (about 18% of them) have incorporated aspects of social media in their business continuity plans.

Although these networks raises additional risks (as shown above) they may prove as useful tools in extreme situations when, for example, communicating with employees following an incident that led to the interruption will be the key element for resuming activities.

2. BUSINESS CONTINUITY PLANNING

Business **C**ontinuity **P**lanning (BCP) is the process created for reducing organization risks from unexpected damage *functions / operations* (manual or automatic) required for the organization survival. The plan includes *procedures* for human resources / materials that support the functions / operations and ensure continuity of service, at the lowest level. *The purpose* of business continuity plan and disaster recovery is that the company would be able to continue its operations and survive the disaster information system outages.

This plan must be *compatible with the company business* and to maintain the general plan of the organization. Such a plan should cover the following unwanted events:

- Certain equipment error (eng, disk crash);
- Power failure or disruption of tele-communications channels;
- Errors or corruption of database applications;
- Employee mistakes or sabotage;
- Attacks of malicious software (viruses, worms, Trojan horses);
- Hacking or other attacks via the Internet;
- Fire;
- Natural disasters (earthquake, flood).

The first step in developing business continuity plan is to improve *risk analysis* (risk identification). The impact analysis shows how great the damage (financial or otherwise) which every risk can generate. Risks must be identified before their impacts [6, 8].

Business continuity plan is more than just an information plan. It identifies how the business will work after the disaster. An important subcomponent of business continuity plan is the plan *Disaster Recovery Planning* (DRP). It contains details of information technology that will be used to restore the system. Plan for disaster recovery may be included in the business continuity plan or can be presented as a separate document, depending on business requirements. DRP addresses the technical aspect of the plan, while BCP takes into consideration the overall operational and business aspect.

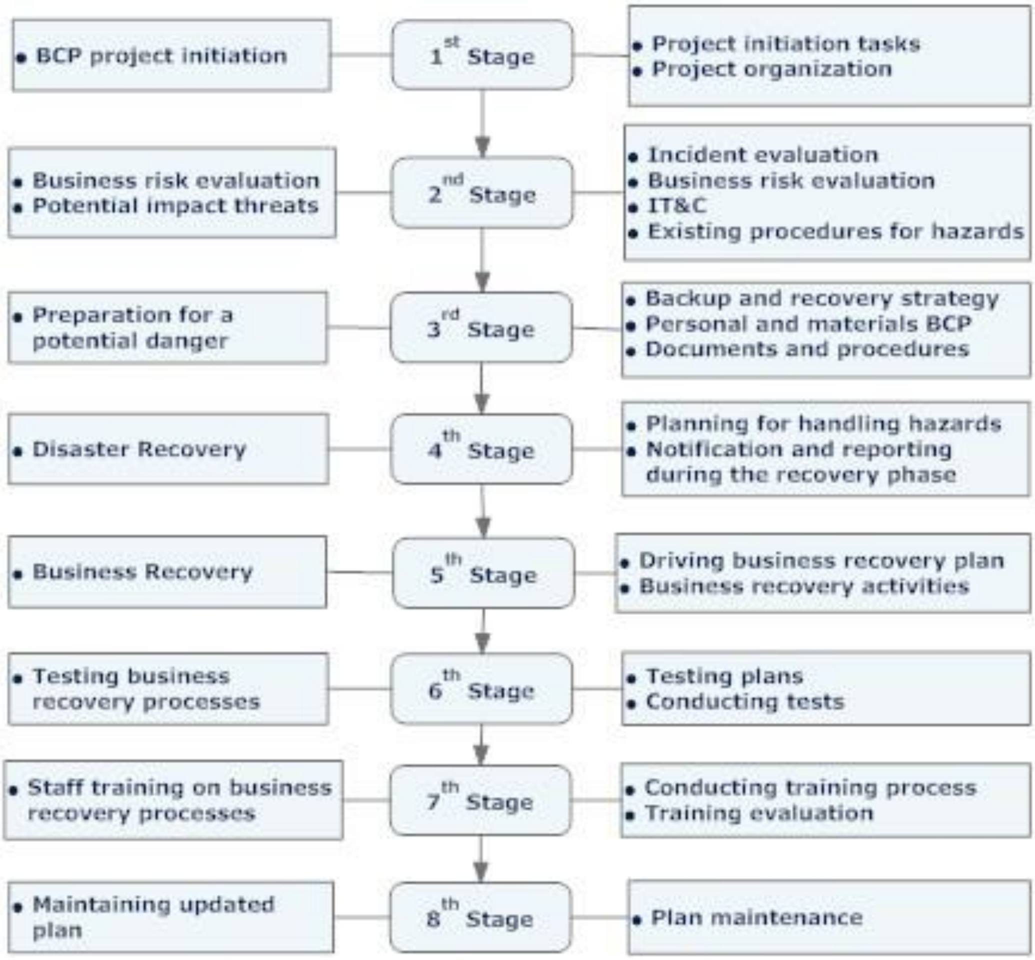
• BCP project initiation
1st Stage
• Project initiation tasks
• Project organization
• Business risk evaluation
• Potential impact threats
2nd Stage
• Incident evaluation
• Business risk evaluation
• IT&C
• Existing procedures for hazards
• Preparation for a potential danger
3rd Stage
• Backup and recovery strategy
• Personal and materials BCP
• Documents and procedures
• Disaster Recovery
4th Stage
• Planning for handling hazards
• Notification and reporting during the recovery phase
• Business Recovery
5th Stage
• Driving business recovery plan
• Business recovery activities
• Testing business recovery processes
6th Stage
• Testing plans
• Conducting tests
• Staff training on business recovery processes
7th Stage
• Conducting training process
• Training evaluation
• Maintaining updated plan
8th Stage
• Plan maintenance

Fig 1. Plan for disaster recovery and business continuity

The next step is the implementation of information by *Business Impact Analysis* (*BIA*). In this phase shall be identified various events that impact on business continuity in the organization in terms of financial, human resources and so on in order to determine critical operations. Next, we will determine the strategies and objectives for critical functions recovery. Finally, it will be necessary to prepare a document on the recovery steps to be followed if an incident is declared.

From logical point of view, business continuity plan should include the following steps:

- *Analysis*, including identification of critical business areas, defining the types of probable attacks and the response scenarios along the agreements on objectives in terms of recovery time and assumed data loss;

- *Design*, involving the definition of the operational structure control, identification and selection of secondary location, communication and switching architecture between locations and agreement on replication methodology and needed software for this operation;
- *Implementation* of the defined solution which includes identifying, completing or expanding areas of responsibility;
- *Testing* or crash and recovery scenarios simulation, which include the achievement of compliance under the original objectives;
- *Maintenance,* which involves periodic testing of the solution (annually or bi-annually) to ensure the continuous operation and maintenance of the solution relative to the compliant changes in business structure or infrastructure.

Ensuring business continuity involves a complex process which contains several components [8]. To have a good plan in place, several aspects should be taken into account:

- *Risk assessment* to which the company is exposed. What are the possible disasters and their occurrence likelihood?
- *The impact* it may have the materialization of each of these risks if the company is not ready.
- What are the *critical infrastructure points* (Single Point of Failure), whose failure would cause the entire network downtime? It is well that these points to be doubled, ensuring in this way the system redundancy. Redundancy can be at the level of equipment (two devices instead of one), at the level of components (two sources, processors and so on) or at the level of application.
- Moreover, with the redundancy, the rapidity with which the transition from one device to another in the event of the failure is important. The majority of solutions can provide an almost imperceptible transition if configured right, ensuring in this way the services continuity.

Recovery strategies can be multiple, depending on the budget available to each company. These may include manual processing, be your own recovery, using multiple locations, the contract with a recovery company, and establish a partnership with client companies.

3. BUSINESS CONTINUITY MANAGEMENT SYSTEMS

Taking into consideration that disruption from natural causes and those caused by human factors continue to have a significant impact on the national and global economy, there is no other better time for adoption of a new international standard for business continuity.
ISO 22301: *Societal security - Business continuity management systems - Requirements* was published by the International Organization for Standardization (ISO) in May 2012 and was designed to provide organizations with adequate instructions for proper implementation of business continuity management systems [9, 10].
The introduction of this standard should provide organizations - partners and stakeholders - a common language, processes and uniform objectives to meet the business continuity challenges in the 21st century.

4. CONCLUSIONS

Business continuity is a serious issue for all organizations regardless of their activity field, in terms of the competitiveness objectives, profitability and market position in which they are running their activities. Capability of an organization to maintain its vital activities after or during a disastrous event and the speed, with which it is able to restore its full functionality, can be the difference between success and failure.
Operational continuity is particularly relevant as the organization operates in exposed to IT risks domains as the financial sector,

telecommunications, utilities and public sector. In this context, well-designed solutions and processes planned for DR / BC become critical to an organization with a modern and complex IT&C infrastructure.

Business continuity program should always remain in the attention of any organization, tested and regularly updated, so that its objectives (eng. business continuity) can still be successfully achieved.

The best way to organize the implementation of business continuity concept is launching of a program inside the organization which allow each organization structure to develop its own project and to contribute to the business continuity plan development, implementation and maintenance. This approach contributes to employee awareness about the importance of the problem [9]. IT&C departments develop plans and procedures for information recovery as part of current professional obligations. These will help anyway in a disaster recovery program plans.

REFERENCES

[1] **Iovan, St. and Ionescu, P.-V.** (2011) *Cloud Computing: A Short Introduction*, Bucharest: Proc. of 12th European Conference (***E_COMM_LINE 2011***), Romania, ISBN-10: 973-1704-20-5;

[2] **Iovan, St. and Ionita, Pr.** (2011) *Breaking into the Clouds*, Bucharest: Proc. of 12th European Conference (***E_COMM_LINE 2011***), Romania, ISBN-10: 973-1704-20-5;

[3] **Iovan, St. and Litra, M.** (2012) *A New Challenge: Large Volumes of Unstructured Data*, Bucharest: Proc. of 13th European Conference (***E_COMM_LINE 2012***), Romania, ISBN-10: 973-1704-22-1;

[4] **Ionescu, P.-V. and Iovan, St.** (2012) *The Adoption of Cloud Computing at the Governmental Level and the Problem of Interoperability*, Bucharest: Proc. of 13th European Conference (***E_COMM_LINE 2012***), Romania, ISBN-10: 973-1704-22-1;

[5] **Iovan, St. and Ionescu, P.-V.** (2012) *Security Issues in Cloud Computing Technology*, Bucharest: Proc. of 13th European Conference (***E_COMM_LINE 2012***), Romania, ISBN-10: 973-1704-22-1;

[6] **Robb, Drew** (2005) *Disaster Recovery Vs. Business Continuity*, 28 aprilie 2005, http://www.esecurityplanet.com/ ;

[7] **Litra, M. and Iovan, St,** (2012) *Innovation Process in Information Technology Used to Support for Business Processes*, Bucharest: Proc. of 13th European Conference (***E_COMM_LINE 2012***), Romania, ISBN-10: 973-1704-22-1;

[8] **Kosutic, Dejan** (2010) *Disaster Recovery Vs. Business Continuity*, 09 noiembrie 2010, http://www.drj.com/

[9] **Ivanus, Cr. and Iovan, St.** (2013) *Providing Products and Services in Cloud Computing Technology*, Bucharest: Proc. of 14th European Conference (***E_COMM_LINE 2013***), România, ISBN-10: 973-1704-22-1;

[10] **Iovan, St. and Ivanus, Cr.** (2013) *Cloud Computing Essential Element – Data Center*, Bucharest: Proc. of 14th European Conference (***E_COMM_LINE 2013***), România, ISBN-10: 973-1704-22-1;