12-2017

Business Continuity and Disaster Recovery Plan for Information Security

Vyshnavi Jorrigala
St. Cloud State University, jvyshnavidevi1277@gmail.com

Business Continuity and Disaster Recovery Plan for Information Security

by

Vyshnavi Devi Jorrigala

A Starred Paper

Submitted to the Graduate Faculty of

Saint Cloud State University

in Partial Fulfillment of the Requirements

for the Degree, of

Master of Science

in Information Assurance

December, 2018

Starred Paper Committee:
Susantha Herath, Chairperson
Dien D. Phan
Balasubramanian Kasi

Abstract

Business continuity planning and Disaster recovery planning are the most crucial elements of a business but are often ignored. Businesses must make a well-structured plan and document for disaster recovery and business continuation, even before a catastrophe occurs. Disasters can be short or may last for a long time, but when an organization is ready for any adversity, it thrives hard and survives. This paper will clearly distinguish the difference between disaster recovery plan and business continuity plan, will describe the components of each plan and finally, will provide an approach that organizations can follow to make better contingency plan so that they will not go out of business when something unexpected happens. This paper will put forward a list of recommendations that an organization can follow to maintain enough strength and resources to react and come out of the crisis successfully.

Acknowledgements

I would like to express my gratitude to everyone who helped me with my starred paper. Firstly, I would like to thank Dr. Susantha Herath, the chairperson of my starred paper committee who have helped me from the beginning of the paper, providing me all the guidance required to start the paper. Besides Dr. Herath, I would also like to thank the rest of the committee members, Dr. Dien D Phan and Dr. Kasi Balasubramanian for being a part of the committee. Thanks to Dr. Dien D Phan and Dr. Abu Hussein Abdullah for their insightful comments.

Thanks to my parents and dearest ones for encouraging me and being my motivation and helping me morally to complete this paper successfully.

Finally, thanking the SCSU library staff for assisting me in fetching and utilizing the resources required to develop a quality work. This paper would not have been possible without the help of each of them mentioned above.

Table of Contents

Chapter Page

Chapter Page

List of Tables

Table Page

List of Figures

Figure Page

Chapter I: Introduction

Introduction

Business requires a number different resources like staff, infrastructure, technology. Most organizations concentrate only on the technological front and expect technology to be the core aspect for success. Although technology is undoubtedly one of the core aspects for success, there are some instances which can break the organization in seconds. Today, small and large business firms rely on the internet, and any disturbance caused to it will halt the major operations and operating areas of that business. Hence, organizations have to be ready for any disturbances in technology that can happen due to unexpected events; the attacks of 9/11 are the best example. A strong and well-structured business continuity and disaster recovery plan would help an organization tackle those unexpected events.

Although there are some organizations that have a good contingency plan ready to help them in critical situations, most of the organizations still do not have a plan, in fact, they do not even bother to have one. It is surprising to know that few organizations do not have strong data back plans set up. A disaster recovery plan or any contingency plan would not help in getting profits for business but would definitely help in preventing losses—huge losses. A disaster can occur at any time, and a business must be prepared for it. “Depending on the nature of the organization and its size and various other factors, a company must design an optimal plan to minimize the effect of disaster and continue the critical business functions” (SANS Institute 2002, p. 559). An optimal plan will consider many factors including the effect and range of the disaster, cost constraints, RTO, RPO, and MTO. This chapter will introduce the problem that has

been the motivation in writing this paper, will explain the nature and significance of the problem, will give an idea on how the research will be progressed and what research questions will be addressed and answered by the end of the paper.

Problem Statement

The main challenge that organizations face while constructing a business continuity and disaster recovery plan is to efficiently prepare, deploy and maintain the plans to avoid the consequences of a disaster.

Nature and Significance of the Problem

Although a good contingency plan in practice would be very beneficial to a company, it is very unfortunate that many businesses do not have it. A disaster can never be expected or detected, even with the high-end technology, and hence we as a company must either be prepared for the disaster or be prepared to shut down the business. Security personnel are accountable for any such circumstances. As the competition is growing, a company cannot just leave themselves behind by not having a good contingency plan. BC and DR plans enhance the responsiveness and guarantee that sensible choices are made by employees during emergencies by providing composed and hazel free techniques to encounter a disaster (Gregg, 2009).

The significance of the problem can be measured by its consequences, and the consequence of a sudden disruption in the services that a business provides are bad reputation, sudden drop in share value, losses in shares, no revenue for the company for specific period and in the worst case, no business at all. “Every two out of five organizations had to shut down

their business within five years of disaster striking" (Wheatman , 2001, ¶1). Even if businesses survive, they have to pay a huge cost for not being prepared for the disaster. After the 9/11 attacks, about 39% of the company's IT budget went to integrating back-end systems, about 24% was used to upgrade IT infrastructure, 34% for new software, and 2% for outsourcing services (Mearian, 2011).

According to Britton (2016), risks of not having a Business Continuity Management Program are:

1. Business Failure: It seems, 75% of the companies drop from their business within three years after a disaster has occurred
2. Disasters can lead to injury and death of the employees, clients and other visitors of the company.
3. Disasters can be very costly, if they are not properly handled. "Over a five-year period, businesses lost more than $70 million due to downtime alone" (Britton, 2016, ¶5).
4. Bad Reputation: Companies that does not have a disaster recovery or a business continuity plan are viewed as insecure investment and untrustworthy by customers and stakeholders.
5. Loss of productivity is the major consequence of disasters, even if the company survives the disaster, it has to compromise on at least one of its mission critical operation.

The problem must be on high priority to initially start with a plan and should always be tested with the current scenarios. Other organizations should be taken as examples, and the documentation should be revised at regular intervals. By having a good contingency plan, employees will have enough knowledge on what choices to be made, what assets to be protected on high priority and which business operation should be continued during a crisis (Gregg, 2009). In other words, organizations have a more controlled procedure to help them come out of a crisis. The study will be useful to know the importance of a disaster recovery and business continuity plan and urges an organization to strictly implement it with all the resources needed.

Objective of the Research

The main objective of the study is to research the concerns related to the implementation of business continuity and disaster recovery plan and provide a best way to prepare and implement both the BC and DR plans.

Study Questions and/or Hypothesis

1. How can an organization make their plan sustainable?
2. What are the best practices to prepare, deploy and maintain a disaster recovery and business continuity plan?
3. What are the different approaches taken by the organization's contingency plan to avoid risks on-site and on cloud?

Limitation of the Research

- Sources are limited.

- Many companies do not disclose their plan and hence resources from online are only used.
- Contingency plan can never be a one-size-fits-all solution.

Definition of Terms

BC: Business Continuity

BCP: Business Continuity Plan

BIA: Business Impact Analysis

BRP: Business Resumption Plan

CP: Contingency Plan

DR: Disaster Recovery

DRP: Disaster Recovery plan

Implementation method: Implementation method is the most the word that is most often used in this paper. The term implementation in this paper is synonymously used for preparing, deploying and maintaining the BC and DR plan.

IR: Incidence Response

MTD: Maximum Tolerable Downtime

RPO: Recovery Point Objective

RTO: Recovery Time Objective

WRT: Work Recovery Time

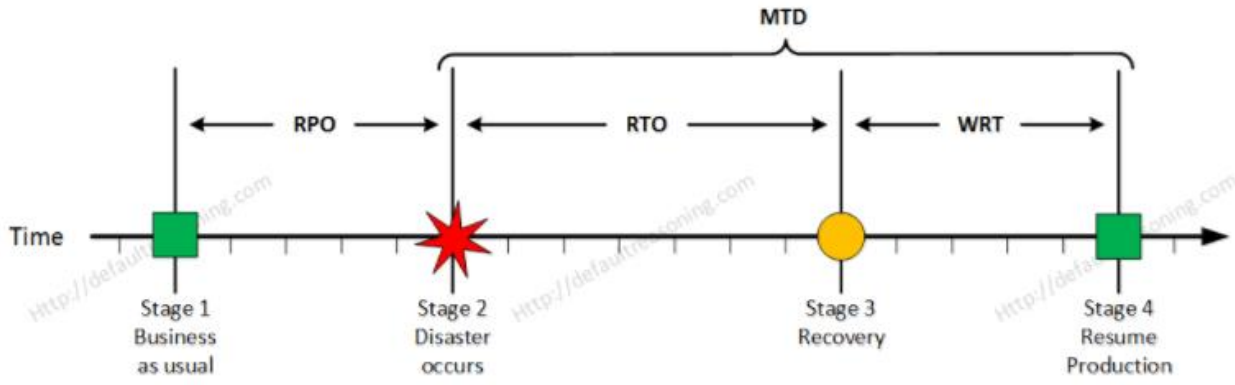


Figure 1. Description of RTO, RPO, MTD, and WRT Pictorially (Marek, 2013)

The above-mentioned abbreviations are the most commonly used terms in the concepts of business continuity/disaster recovery/ business continuity plan document/disaster recovery plan document.

Summary

This chapter has covered the introduction to the research on BC and DR plan implementation. The need and importance of having those plans in an organization, shortcomings of organizations in having a good contingency plan and consequences of not being prepared for a disaster are put forth in this chapter. Definition of a few terms used in this paper are explained in this chapter. Further, the objective and main problem that has been the driving force for the research are also discussed along with questions that will be addressed as a part of this research.

Chapter II: Background and Review of Literature

Introduction

From the day the internet became the vital component of operating a business, attacks on compromising systems with networks as the main vulnerable tool have begun. While cyber-attacks are the most certain aspects that come into mind when thought about information security, there are some attacks that are not intentionally done yet bring huge losses to the organization. Either way, businesses must prepare themselves for the disaster. “The secret of survival is preparation” (Edwards, 1994, p. 38). BCP and DRP are the data security solutions for businesses when unexpected events happen. Most of the times BCP and DRP are misunderstood to be one and the same, but there is a clear difference between both. This chapter will give a brief introduction about the contingency plan, more specifically BC and DR plans and the differences between them. Literature related to the problem and the methods addressed by different researchers are put forth in this chapter. This chapter will give an idea about the shortcomings of the current approach of building a business continuity and disaster recovery plan that can help in building a better and successful plan.

Background Related to the Problem

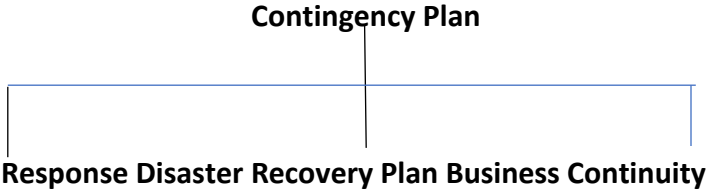
Disaster is the most common word used in this paper and, before any assumption is made in understanding what a disaster is, and concluding only natural disasters like volcanic eruptions, earthquake, tsunamis to be disasters, the following will give an understanding of the reasons behind disasters.

Disasters can be caused because of environmental conditions, system failure or equipment failure or disasters can also be man-made. Any incident that can take more than acceptable amount of time to recover or if it has more than acceptable range of consequences, can be called as disaster.

- Cooling plant failure
- Cyber attacks
- Disasters caused because of equipment failure:
- Disasters caused by environmental conditions:
- Disasters caused by human:
- Earthquake
- Hurricanes
- Landslides etc.
- Mischievous activity by disgruntled employee
- Power failure or power outages
- Sabotage
- Security breaches:
- Sensitive information disclosure etc.
- Sink holes
- System damage etc.
- Terrorist attack
- Theft etc.

- Thunders/electrical storms
- Tsunami
- Volcanic eruption
- War

Going back to the history, when an adverse event occurs and the data or records or equipment are damaged, the result cannot be undone, and the business is either on halt or put to an end. But, as the technology has grown, many data back up plans have come up so that at least the data and information are not lost. Adding to the benefit of having the ability to bring the data back, if a business can also run its core processes during the disasters, will be the great capability one can bring into this digital era. That capability is called the Contingency plan, which includes incident response, disaster recovery and business continuity plans.



Incident response. Incident response is a phase that prepares a team, Incident Response Team, to be ready to handle any incident on the moment. An incident can range from hardware failure or power outages to violation of organization's policies by a disgruntled employee (Bejtlich, 2004). Incident response team's work will help an organization to identify how well a team is working to handle the improper functioning sections in an organization.

Disaster recovery plan. Disaster Recovery Plan is a plan designed to recover all the vital business processes during a disaster with in a limited amount of time. This plan has all the

procedures required to handle the emergency situations. A disaster recovery process should have provable recovery capability, and hence it provides the most efficient method to be adopted immediately after a disaster occurs. Mostly the DRP has technology oriented methodologies and concentrates on getting the systems up as soon as possible, within a reasonable amount of time (RTO and RPO). RTO and RPO are the recovery time objective and recovery point objective, which are the targets of DRP. "The most successful disaster recovery strategy is the one that will never be implemented; therefore, risk avoidance is a critical element in the disaster recovery process" (Martin, 2002, p. 1).

Business continuity plan. "Business continuity refers to the activities required to keep the organization running during a period of displacement or interruption of normal operations" (SANS Institute, 2002, p. 1). BCP helps in continuing the business even after a disaster occurs. Business has to stay active during the crisis; if it closes its operations even for a day or a week, they are many chances that the organization will experience losses and will have to shut down. Moreover, legal issues can arise if the critical services are not provided to clients. This can lead to bad reputation and many more legal problems for an organization in addition to having the pain of being in the state of disaster. Hence an efficient BCP plan can be used to actively run and maintain the business activities.

Differences between disaster recovery and business continuity plan. Most of the organizations assume that business continuity and disaster recovery plans are one and the same and efforts of preparing the plan should not be doubled by having two different plans for DR and BC. The terms business continuity and disaster recovery always come together, this is

because they are meant to be done parallelly and are not synonyms. Understanding differences between both the plans and having them done individually yet parallelly will help organizations to have a different view on results of both the plans. Table1 shows the differences between BCP and DRP.

Table 1

Differences between DRP and BCP

Disaster Recovery Plan	Business Continuity Plan
Activities are pre-planned to react to disasters.	Planning on mitigating risk for the assets, business processes that will adversely impact company, if a disaster happens.
DR plan starts with IT, not because other aspects are not important, but because IT is easiest to recover, and impact is also more.	BC plan is not an IT process; it includes the complete business as a unit.
A DR plan can be built upon a strong business continuity plan.	The business continuity process has a series of DRPs.
Disaster recovery is data centric.	Business continuity is business centric.
Main idea: Recover from disasters.	Main idea: Continue critical business operations.

Contingency planning, more precisely business continuity and disaster recovery plans, decides the last chance for a business to survive. Global Benchmark Study reveals that 73% of the organizations lack disaster recovery strategies and more than 5 million losses are incurred due to critical application failure, data losses, data center outages etc. (Kahan, 2014). Figure 2 illustrates the massive losses incurred by organizations/companies/countries due to natural calamities causing economic, human, technological damage.

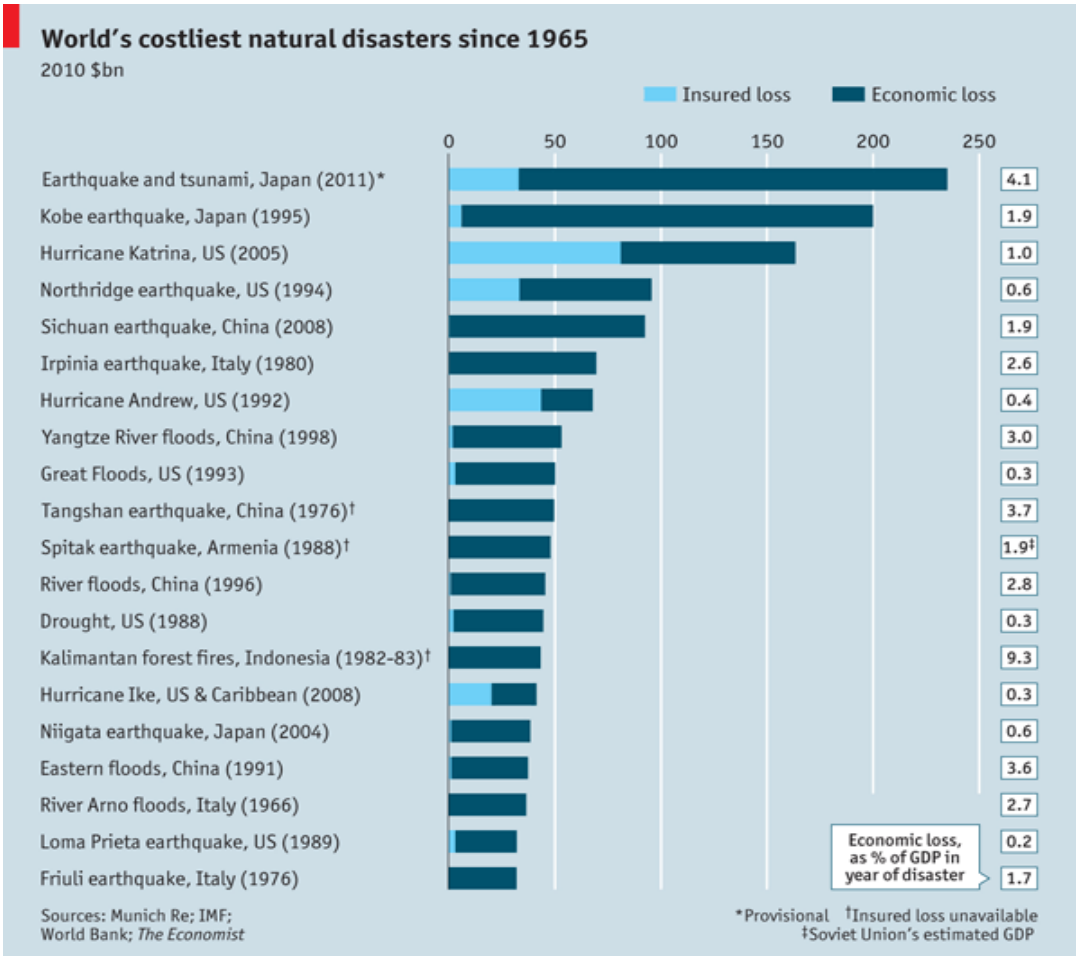


Figure 2. Losses Incurred Due to Natural Disaster (Economist, 2011)

It can be seen from the above figure that, the economic and uninsured losses due to tsunami and earthquake in 2011, in Japan was nearly $230 billion, resulting in 4.1% of GDP loss for that year.

The organizations that thought ahead and had a plan that is prepared for the impacts of a disaster survive in this competitive world. There are very few such organizations, statistically only 5% of the organizations are genuinely prepared to handle a disaster.

Organization's concerns in creating and updating BC and DR plans.

192 Enterprises Surveyed January to July 2016		
	Count	Percent
Error in Plan	122	64%
Plan not up to date	91	47%
No major issues with plan	87	45%
Unable to find password	66	34%
Security blocked implementation	47	24%
Insufficient training	45	23%
Insufficient backup power	41	21%
Compunction network missing / failure	39	20%
Plan not documented	27	14%
Recovery priorities not identified	26	14%
Plan did not cover ransomware attack	21	11%
Event not identified (in time)	21	11%

Figure 3. Disaster Recovery Business Continuity Planning Template (Prleap, 2016)

Figure 3 shows the analysis of a survey conducted by Janco Associates (Prleap, 2016) to understand why disaster recovery plans of many organizations fail. The survey was conducted on 253 enterprises which had to use their plan to recover from disaster but have failed to achieve success in the recovery process.

From the above statistics given by Janco Associates (Prleap, 2016) on DR and BC plan focusing ransomware, it is evident that not many organizations have their plans up to date, moreover some of them are erroneous and many other issues can be pointed out.

One of the concerns specified by few of the organizations was that, it was difficult to update plans as they were purely in written format (Prleap, 2016).

One other reason for companies being reluctant to test their plans is that, full scenario testing is time consuming and expensive (Kamath, 2007).

Literature Related to the Problem

The main reason organizations put forth for not having a DRP or BCP is the inadequacy of resources. But the question here is, what if an unforeseen incident happens? No matter how big an organization is, if any occurrence could bring its everyday operations to a halt and it does not have an alternative plan (that we call DRP and BCP plans here), it will have irrecoverable losses. The need for DRP or BCP cannot be exaggerated, but after the September 11, 2001 incident, it was very clear that although the probability of occurrence of an event is low, the impact will be very high and can only be tackled with a well-structured contingency plan. Almost half of the medium sized enterprises did not trade again after they are affected by 9/11 attacks (Kamath, 2007).

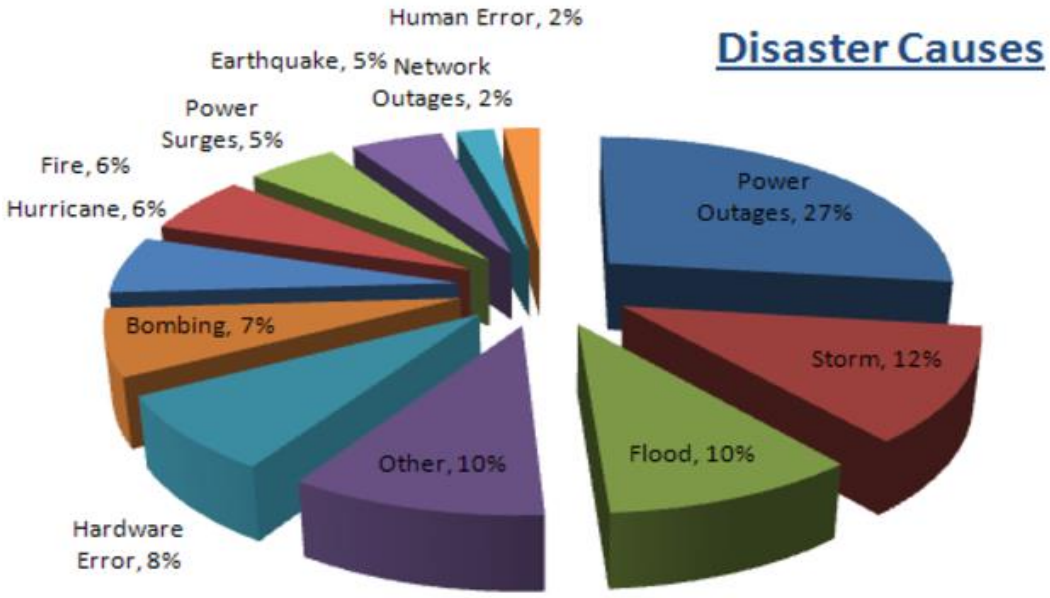


Figure 4. Causes of Disasters (Telovations, 2012)

From Figure 4, there are several different ways in which a disaster can occur. This means there are several different hosts that are ready to shut down your business, if not shutdown, these disasters can succeed in disrupting the business operations for some period which can result in losing of profits, clients, company reputation and many others. Companies should consider having business continuity and disaster recovery plan very seriously as we never know which incident can become a disaster or which disaster can occur at the next moment and a good plan can always increase the chances of saving the company from a disaster.

According to Widup (2003), "20.4% of the organization does not have a disaster recovery plan, among the organizations that have DRP, 26.1% of them have not tested their plan" (p. 1).

According to Snedaker (2007), BC and DR plans cannot be ignored as the statistics of losses due to disaster are alarming and this should serve as a wakeup call for IT professionals and corporate executives.

After the September 11, 2001 horrifying terrorist attacks on the World Trade Center, government agencies and businesses have decided to implement DR plans to strengthen security and business continuity. Immediately after the attack, 73 declarations from 36 companies seeking help were filed regarding the disaster (Hanning, 2001).

A disaster recovery plan is much more than just having data backups, and most of the organizations having this misconception have changed their minds after September 11 (Lancaster, 2002).

"Business continuity and disaster recovery are the strategies implemented to increase the likelihood of effectively recovering business functions from a major disaster" (Barbara, 2006, p. iii).

Nations	National Regulations	Organization	Information Security Management	IT Disaster Recovery Plan	DC Management	Telecommunications
US	NIST Special Publication 800-34(SP 800-34)—Contingency Planning Guide for Federal Information Systems	National Institute of Standards and Technology, NIST	V	V		
	Telecommunications Infrastructure Standard for Data Centers:TIA-942	American National Standards Institute, ANSI	V	V	V	V
Japan	Data Center Facility Standard	Japan Data Center Council, JDCC		V	V	
Korea	TTAS.KO-10.0259 on Guidelines for Disaster Management of Information Systems	Telecommunication and Technology Association, TTA	V	V		
Taiwan	Information Security Management Directions for the Executive Yuan and its Subordinate Agencies	Executive Yuan	V	V		
	CNS27001: Information technology—Security techniques—Information security management systems -Requirements	Bureau of Standards Metrology and Inspection, MOEA	V	V		
	The norms of Information and Communication Security Management in Educational Systems	Ministry of Education	V	V		
Saudi Arabia	Guidelines on disaster recovery Planning for ICT Industry	Communications and Information Technology Commission, CITC		V		V

Figure 5. *Regulations for Disaster Recovery Sites by Different Countries* (Yang, Yuan, & Huang, 2015)

Figure 5 shows the disaster recovery regulations given by governments of different countries. The paper given by Yang et al. (2015) concentrates on choosing of disaster recovery sites which is very important to continue the business operations even after the disaster.

Literature Related to the Methodology

Organizations build their DRP and BC plans in different ways, applying different standards, best practices, methods that come from disaster experiences of other organizations, or some perception of what could happen. The chart below shows the concentration of various standards on creating a BC plan.

Standards referred below are:

FFIEC: Federal Financial Institutions Examination Council

NFPA 1600: National Fire Protection Association

NIST: National Institute of Standards and Technology

FERC: Federal Energy Regulatory Commission

GTAG: Global Technology Audit Guide

ISO 22301: International Standards Organization

HIPPA: Health Insurance Portability and Accountability

FFIEC	NFPA 1600	NIST	FERC	GTAG	ISO 22301	HIPAA	TOTAL
1. PROGRAM ORGANIZATION, MANAGEMENT & TRAINING							
8	12	7	3	5	10	0	12
2. BUSINESS IMPACT ANALYSIS (BIA)							
6	4	8	4	8	7	3	9
3. EMERGENCY RESPONSE & CRISIS MANAGEMENT							
18	26	19	19	16	16	1	31
4. EMERGENCY FACILITIES							
12	6	3	1	5	1	0	12
5. BUSINESS & IT RECOVERY							
14	7	8	4	8	5	3	16
6. TESTING							
13	14	13	1	10	8	1	14
7. MAINTENANCE							
3	0	3	1	2	4	1	4
8. AUDIT & GENERAL POLICY							
2	0	2	0	1	3	0	3
TOTAL							
76	**69**	**63**	**33**	**55**	**54**	**9**	**101**

Figure 6. BC Focus Points of Various Standards (Disaster Standards, n.d.)

From Figure 6, each standard has a different approach towards BC plan as each of them has a different perspective of what is important. From Figure 3, it can be observed that NFPA 1600 standard is more focused on emergency response and crisis management but has zero focus on maintenance, audit and general policy. When an organization considers only NFPA 1600 standard while preparing its BC plan, the plan will do well in performing emergency response operations and crisis management, but it will not have any process to maintain or audit the BC plan. Hence, when developing a plan, it is important to understand that following only one standard will not help.

Any methodology that used by the organization should be planned, developed, tested, and implemented. The following are assessed to be the key elements to implement a disaster recovery plan:

- Critical applications must be assessed.

- Procedures must be developed to get data back-up.
- Procedures must be developed for recovery operations.
- Implement all the procedures developed.
- Test procedures.
- Plan for the maintenance of those procedures (Martin,2002).

The Business Continuity Plan includes the following:

- Governance of BCP.
- Business Impact Analysis (BIA).
- Planning for the measure to be taken and arrangements for BCP.
- Dependency on the readiness of the procedures.
- Exercising, maintaining and auditing the plan. (Public Safety Canada, 2015).

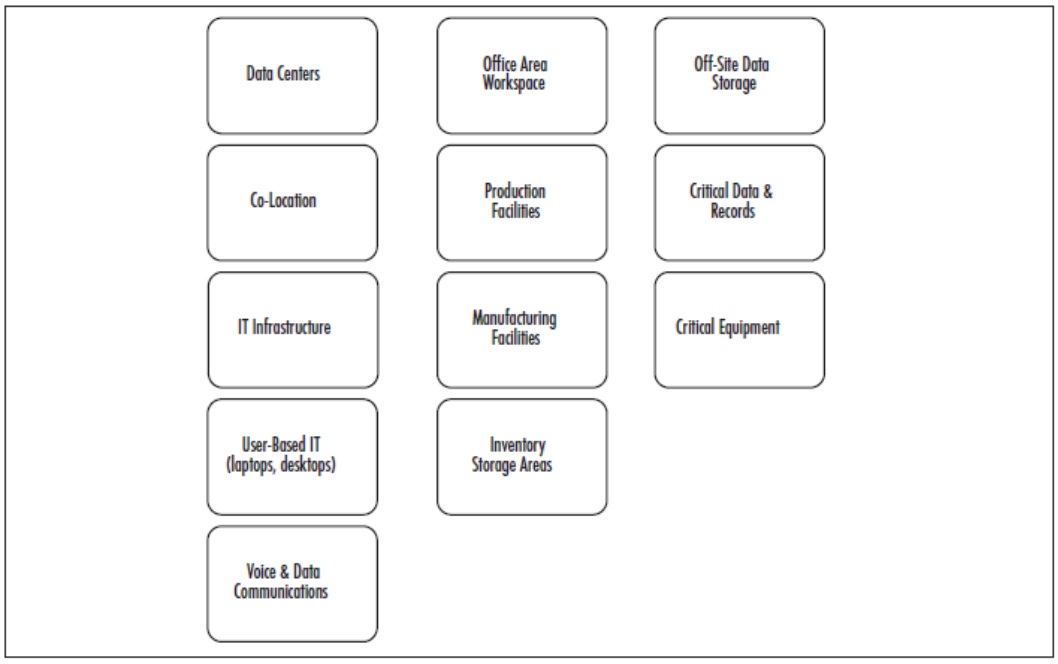


Figure 7. Critical Elements of BC and DR Plans (Snedaker, 2007)

ISO 22301 has given the latest BC standard called “Societal Security–Business Continuity Management Systems–Requirements” which says, Plan-Act-Do-Check as the way a BC plan must be implemented (Janco Associates, n.d.). The Disaster recovery and Business Continuity template of Janco Associates (n.d.) is as follows:

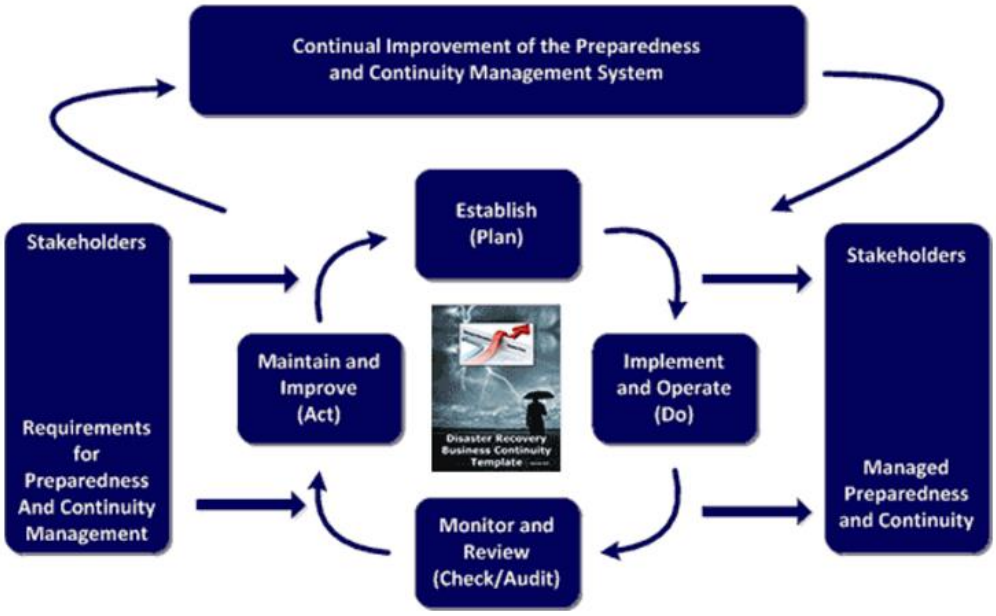


Figure 8. Business Continuity and Disaster Recovery Template (Janco Associates, n.d.)

From Figure 5, it is very clear that not all standards are focused on all the critical aspects of a BC or a DR plan and following only one standard’s best practices to build either DR or BC plan would mean that some of the critical aspects of the plan are missed. Most of the times, if an organization could not provide the services to a client due to a disaster and if the organization is unable to show its client that it has put all its efforts for a disaster recovery and business continuity then it will have to face the legal consequences.

The following is the methodology used to develop business continuity plan by UK-based multi-national banking group which is Standard Chartered Bank. Because of IRA terrorist attacks in London and its consequences on Standard Chartered bank twice in 1992 and 1993, Bank of England has directed SCB to develop business continuity plan. Creation of organizational level and individual plans (department level) and integrating them was the methodology followed by SCB.

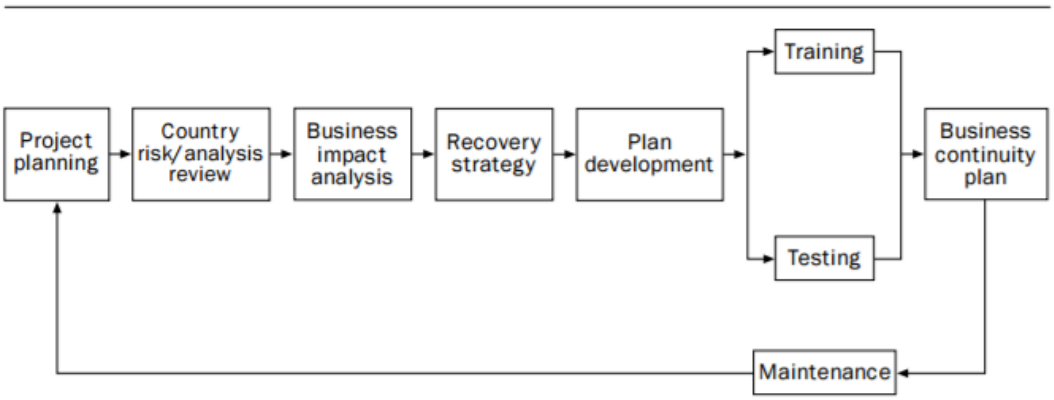


Figure 9. BCP Plan by SCB (Heng, 1996)

Scope of the plan, objectives, and assumptions are provided before the development of the plan is initiated.

1. During project planning, resources required for the project, project duration and project commencement dates are fixed by negotiating with the management.
2. Business impact analysis: This step involves performing business impact analysis, analyzing risk and determining minimum requirement for processing.

3. Recovery strategy: Recovery strategies will be developed during this phase to recover the vital business processes, to back up data and select alternatives for the recovery process.
4. Plan development: Business continuity planning software is used to develop templates for the plan which are then customized. The plan includes emergency response, business and support functions recovery planning.
5. Testing: Testing is done after the first iteration of development phase, and training is done as part of testing.

Summary

These days, businesses do not compromise on anything that comes in their way of effective performance; then why are BC and DR plans left undone? Also, most of the companies assume that BC and DR plans are one and the same. This chapter helps understand the basic idea of having a different business continuity plan, disaster recovery plan and put forward the differences between them. This chapter also includes the literature review of the problem which is the need and implementation of business continuity plan and the review on methodology used by different organizations as a part of their planning for the disaster.

Chapter III: Methodology

Introduction

The methodology and perspective of the organization towards developing a plan is critical to the outcome of BC and DR plans. It should be noted that an incomplete or a bad plan is more dangerous than having no plan at all. A plan that is not sufficiently analyzed or tested can misguide the employees at the time of crisis. Moreover, the cost and effort used in preparing a plan goes in vain if it is does not help in crisis. Therefore, following an appropriate method and best practices that are most suitable to the organization's needs is very important. This chapter will discuss the methodology used to perform the research and the resources used to collect information for the research.

Design of Study

This study mainly involves research of the effective implementation of business continuity and disaster recovery plans. The research questions mentioned previously in the paper will be analyzed and answered by carefully studying and exploring a number of research sources. Company websites, SCSU library website's database, journals and articles that are credible and peer reviewed will be the main sources for this research. The paper is divided into three parts:

1. Research the concerns of the organizations in having a disaster recovery and business continuity plan.
2. Deduce best practices from different standards that provide best practices for business continuity and disaster recovery plan, as mentioned previously in chapter

2, various standards that gave best practices for business continuity planning have different perspective over which aspect of a BCP is important and hence this paper will research will examine various standards and devise best practices that concentrates on all the aspects of BCP and DRP.

3. An implementation method for a successful and sustainable BCP and DRP will be given by the end of the research.

An implementation method that will be most appropriate to strategically plan for a disaster will be put forth in this paper along with the explanation of why this method is most appropriate. The implementation method will be deduced by carefully examining the best practices given by various standards and analyzing the BC and DR plans that are currently used by a few chosen organizations or the templates provided. Some of the success factors for BC and DR plans are:

- How is criticality of business functions identified?
- How Risk Assessment is done?
- How Roles and responsibilities are assigned?
- Is testing done at regular intervals?
- Coordinating in tasks during and after the disaster?
- How do they define RTO, RPO, MTD?
- How geographically scattered are the sources of organization?
- Training of personnel for handling critical situations.

- Undoubtedly, having a backup plan is the first and the most basic aspect of tackling a disaster.
- Scalability of the plans to accommodate the newly uncovered disasters.
- Maintenance of the plans in the form of electronic documents and templates.
- How realistic deadlines and outputs are estimated by the organization.

The research will give IT managers an insight on what decision to make during a crisis and will also explore the reasons for organizations not implementing DR and BC plans. The approach of this paper is more qualitative as it researches on the process or the procedure to be adopted for preparing an effective DR and BC plan.

Data Collection

The information collected during this research will be from company websites, SCSU library, articles, Business Continuity Plan service providers and leading companies, Disaster Recovery Journal and other journals, surveys reports on business continuity and disaster recovery, and various standards as specified previously in the paper. Most of the information collected will be from web, as many organizations are not ready to reveal their plans to outsiders.

Data Analysis

The research questions mentioned in Chapter I will be analyzed and answered after carefully studying and exploring many sources from online i.e., survey papers, company websites, white papers, journals, and service providers as Janco Associates previously mentioned in this paper etc.

Steps to complete the research:

1. Answering Research Question 1: How can an organization make their plan sustainable and launch it?

   Business continuity and disaster recovery plans are comparatively new topics and have very limited publications that are totally focused on these plans. Hence, journals and white papers are taken an authoritative source for the most part of this paper. “Sustainable business continuity plan,” “sustainable BCP and DRP,” “sustainable DRP,” and “sustainable BCP” are the keywords used for the internet search and has resulted in almost 65,000 results with articles, journals, and white papers related to how to sustain BCP or DRP and what are the factors that need to be considered to make a sustainable plan. From the results generated by these key words, relevant documents and articles are gathered for the qualitative research and the Research Question 1 is answered.

2. Answering Research Question 2: What are the best practices to prepare, deploy and maintain a disaster recovery and business continuity plan?

   To answer this question, research will be done in such a way that data gathered from different sources is reviewed and focused to get the results for business continuity and disaster recovery. Websites and journals that are credible are chosen as information sources.

   To answer this question effectively, firstly an organization or the reader has to understand the importance of BCP and DRP and the devastating results of the lack of

these plans. Importance and consequences of lack of BCP and DRP are shown in the earlier in this paper, the later section to answer this question will contain different phases that are undergone to implement BCP and DRP effectively. These phases are based on the studies conducted using resources from web and SCSU library.

Terms Concatenated to the Word Disaster Recovery for the Web Search	Terms Concatenated to the Word Business Continuity for the Web Search
1. Information System (*)	1. Technology
2. Strategies	2. Principle
3. Technology	3. Information Management
4. Plan Implementation	4. Information Security
5. Plan*	5. Plan*
	6. Information Availability

3. Answering Research Question 3: What are the different approaches taken by the organization's contingency plan to avoid risks on-site and on cloud?

   The research results are fueled by learning the ideas from various articles and white papers written by many information security professionals, CEO's and business continuity and disaster recovery specialists of various organizations. From the results of the web search, credible and relevant resources are gathered and a research on the ongoing risks associated with cloud are looked for and based on the risks and the benefits that cloud bring to the organization, three methods are proposed to have either the data back up or business continuity plan or the disaster recovery plan to reside on cloud.

Summary

This chapter starts with a brief introduction of the importance of methodology used in creating business continuity and disaster recovery plan and will continue to provide the design of study and the methodology used to perform the research to give best practices and best implementation method for a BC plan and a DR plan that a company can rely upon. The sources from which the research is done till now and what other sources will be used in future to perform the research are mentioned in this chapter.

Chapter IV: Analysis of Results

Introduction

Any organization in the world will have some core processes, that when ceased or, are inaccessible for some unacceptable period, will jeopardize its business. The damages caused to the reputation, economy is frightening. With all the daily reports on natural calamities, disgruntled employees, cyberattacks on individuals, government and non-government organizations, it is implied that an integrated and holistic framework is needed to mitigate risks and identify responses, evaluate them to suite the risk circumstances (Berman, 2015). Hence, to remain safe and have seamless business operation's continuity, organizations must build a strong business continuity and disaster recovery plan and strictly implement it. This chapter will provide the results of the research, the research questions mentioned in the beginning of the paper will be answered as part of results and data presentation.

Data Presentation

Business continuity plan holds the biggest place in the context of contingency plan while disaster recovery plan and enterprise risk management are the parts of BCP. Disaster recovery plan concentrates on restoring the IT framework, Enterprise risk management concentrates on anticipating and mitigating the risks that organization might face so that strategies can be developed to minimize the impact of the risk. Business continuity, when looking at the big picture, has disaster recovery plan and risk management involved in it and hence planning for a DRP and ERM will make the way for BCP.

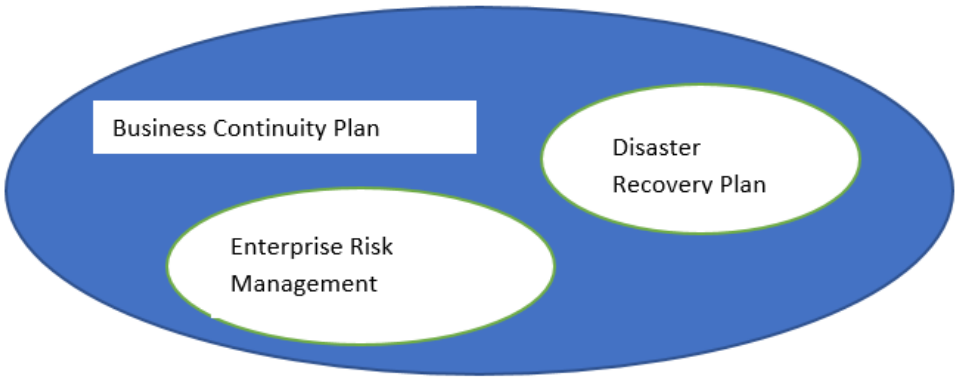


Figure 10. Disaster Recovery and Enterprise Business Management as Part of a Business Continuity Plan

Table 2

Difference between Risk Management, Emergency Response, and Business Continuity

Risk Management	Emergency Response	Business Continuity
What could happen?	What if it happened?	What next?
Identify hazards and opportunities.	Stabilize conditions following a risk event and minimize negative effects	Reestablish sufficient services to permit continued mission essential operations following a risk event.

Research Question 1. *How can an organization make their plan sustainable and launch it?* Downtimes are costly and are risk to the brand name, reputation, budget, focus, vulnerabilities and many other aspects related to an enterprise. During tough times, the capability and resiliency of the organization will only depend on how sustainable its business continuity plan is. A sustainable plan is reliable and will improve a company's resiliency.

***Successful plan*.** Things to be considered while launching a to-be successful BC and DR plan include:

- Organizational Policies and Compliance requirements
- Various modifications to the structure and development of the organization
- Findings, discrepancies in previous audits
- Lessons learned from the kind of hurdles your and other organizations have faced, how the crisis was tackled, drawbacks and success stories.
- Challenges that constrain the plans like lack of proper resources, perception of what could happen and what might happen in real may vary, commitment to time and budget etc.

Plan objectives. The objectives of the plan are (a) to make the continuity and recovery process painless, and (b) get the business on board.

Following are the high-level roles and responsibilities that are set as the basis for the segregation of duties for BC and DR team. Dividing the tasks and assigning the roles and responsibilities for an employee or a group of them will give more power to lead the plan to success. With roles and responsibilities properly assigned, there will be no ambiguities on who does what and who has the ownership and responsibility of what.

Role	Responsibility
DR/BC Services	• Educate and Train • Lead and Provide Guidance • Coordinate Execution of BC Initiative • Perform Risk Assessment and Gap Analysis • Coordinate Executive Review and Validation of Recovery Priorities
Business Sponsor/Single Point of Contact	• Liaison between DR/BC Services and Business Area • Expert Level of Knowledge of Business Area • Identifies Stakeholders Within Organization • Provides Overall Support and Guidance
Business Department/Functional Owner	• Ownership of BC Within Respective Business Function • Reviews and Approves BIA output • Reviews and Approves BC Plan • Participates in BC Exercises
Business Department/Functional Administrator	• Maintains and Updates BC Within Respective Business Function (BIA, BC Planning) • Participates in BC Exercises

Figure 11. Roles and Responsibilities of DR and BC Personnel (Lucht, 2014)

Figure 12. Business Continuity Life Cycle (Lucht, 2014)

***Business impact analysis*.** "The Business Impact Analysis (BIA) focuses on the effects or consequences of the interruption to critical business functions and attempts to quantify the financial and non-financial costs associated with a disaster" (Rouse, 2015, ¶3). BIA defines the Recovery Time Objective (RTO) and Recovery Point Objective (RPO). BIA, if done prior to the disaster or crisis, will help the organization in having a smoother recovery process.

Relationship between disruptive events and BIA

EVENT	TECHNOLOGY ELEMENTS AFFECTED	BUSINESS ACTIVITY AFFECTED	POTENTIAL OPERATIONAL LOSS	POTENTIAL FINANCIAL LOSS	MINIMUM TIME NEEDED TO RECOVER
Fire in data center	IT systems, networks, apps, data	Processes supported by IT systems	Inability of the business to function normally	$3,000-$10,000 per hour	3-4 hours to 1-2 days
Loss of critical servers	Specific servers	Activities that are supported by those servers	Cannot perform specific business processes	$2,000-$5,000 per hour	3-4 hours
Loss of DBMS *(database management system) administrator*	Database management systems	Activities that need specific DBMS	Reduced ability to provide DBMS management	None, assuming backup staff or third-party vendor support available	None to 1-2 days

Figure 13. BIA and Disruptive Events Relationship (Kirvan, 2015)

Risk assessment and gap analysis. According to Kirvan (2015) when commenting on the Risk Assessment, "The risk analysis helps you with identifying possible risks and vulnerabilities that could disturb the continued operation of the BIA-distinguished processes and systems."

Gap Analysis, on the other hand, does the math on the desired performance levels and actual performance levels so that organization can find the gaps in the existing system and conduct programs or activities to fill those gaps.

Plan development. Plan development is essential for the success of both business continuity and disaster recovery operations. Proper planning for emergencies will lead to

smoother recoveries and less hardships. Costs related to the recovery procedures, recovery times, losses can be reduced significantly if there is a proper plan at place.

Testing. While testing is the easiest job and the most underrated job, there are many cases of having a software failure only because the software was not tested for its basic functionality. Lack of testing results in an illusion of having everything perfect and ready for deployment, but in real, nothing is perfect. Same formula goes for disaster recovery and business continuity planning. Every action during a recovery should be simulated with good amount of resources, equipment, supplies as would be used during the emergency, following the procedure as planned. DRP and BCP must be tested in the same way as any application or software program will be tested to find the shortcomings and every output should be documented along with the dates, assumptions, limitations, requirements etc.

Research Question 2. *What are the best practices to prepare, deploy and maintain a disaster recovery and business continuity plan? The best practices to prepare, deploy and* maintain a disaster recovery and business continuity plan are accumulated based on the following questions i.e., best practices will have criteria that can answer the following questions.

- How to identify the risks or possible risks/ disasters?
- How to identify the assets the keeps the business running during disaster?
- How to identify the key resources in the organization?
- How to assign roles and responsibilities for the key personnel of the organization?
- How to communicate during the crisis, both internally and externally?

The structure of the BC and DR plans are divided into three parts: Plan, Implement, and Follow Up.

***Phase 1—Plan*.** During this phase, an organization is far ahead of having a possibility of disaster because, "The onset of a disaster is not the time to plan. Rather, smart businesses take a proactive stance, from the CEO on down, making Business Continuity a priority for the entire organization" (Pitney Bowes, n.d., p. 3). Planning should be the first step and it starts by acknowledging the vulnerabilities, risks and requirements of the organization. Business impact analysis and risk assessment plays a critical role in this phase. "Business impact analysis is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of disaster, accident or emergency" (Rouse, 2015, ¶4)

Risk assessment is the first step of organizational risk management and it will provide the organization with all the possible risks that can come on the way to hinder the business operations. "Project risk management is the art and science of identifying, analyzing and responding to risk throughout the life of a project and in the best interests of meeting project objectives" (Schwalbe, 2015, p. 4). While risk assessment unveils the risks that might occur, business impact analysis will give the details of how quick the recovery activities should work to minimize the losses.

Table 3

Threats that Can Come from Software

Threat	Description of Threat	Mitigating Method
Injection	Injection defects will empower the hacker to bypass application access controls and make, change, erase or read information the application can get to.	Require proper input validation, and verify all data that is received. This prevents malicious data from being entered into a target application.
Broken authentication and session management	Compromised validation procedures lead to information leakage	Create strong passwords
Cross-site scripting (xss)	Harmful scripts are applied to the web server, however they keep running on the customer browser with XSS, attempts are made to execute this dangerous code by injection and running it on the customer browser.	Train users in how to detect and identify suspicious links, which can restrict the access to high risk sites.
Security misconfiguration	Applications or hardware might have improper settings and configurations which can lead to serious risks.	Try to remove or control access to non-essential applications.

(Harwood, 2015)

Risk assessment. According to the ISO 27001 and ISO 22301, risk assessment is mandatory for every organization. The first step in risk management is to assess risk and there are three steps to assess risk within an organization, define, rate, and report (Scofield & Martinez, 2011).

- Define. In this step, risks across all the departments of an organization are identified. The risks associated with key business operations are identified and classified based on the factors that can cause risk.

- Rate. Make a cartesian product of the risks and compare each risk with every other risk and provide a numerical value for the possibility of the risk and possible impact of each risk. Provide a value for the comparison of one risk to another. When a numerical value is assigned to the risk by giving the meaning of the numerical value as 1 as least likely to 5 as most likely, it will be very easy to assess which asset has more risk and the probability that the risk might happen in near future. More importance can be given to those assets and business functions at the time of crisis instead of wasting time on saving the resources that are least useful in business continuity.
- Report. Providing a comprehensive list of the risks and numerical values associated with them, that describes the impact and possibility of risk occurrence in a standard format to the authorities, in a way that is easy to understand. This will help the decision makers to prioritize risks and more efficiently allocate resources to manage and mitigate the risks.

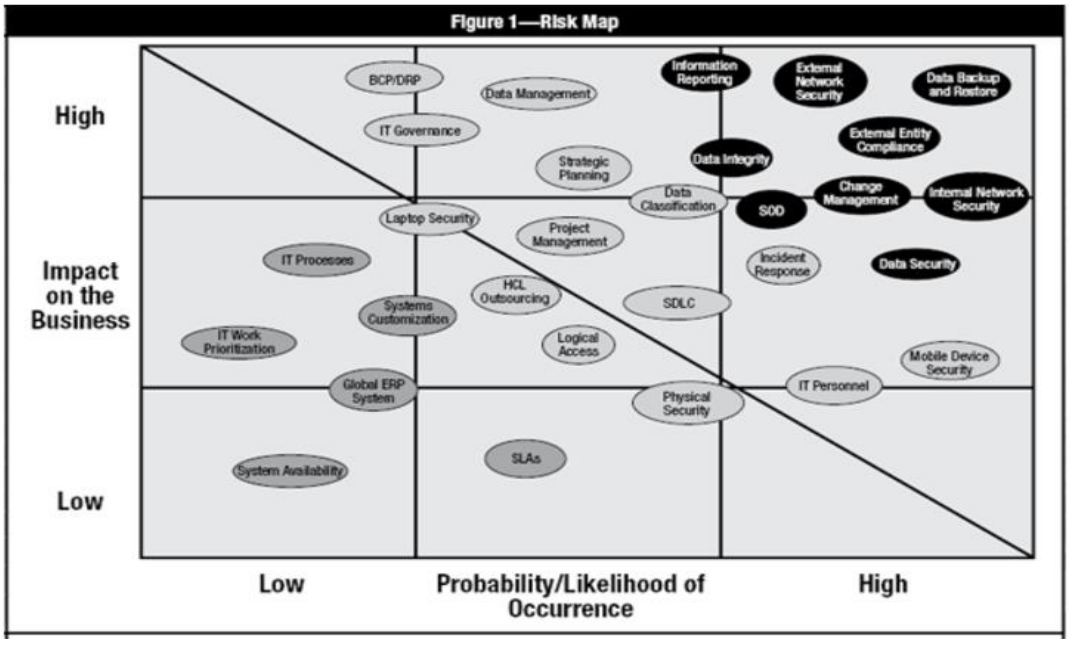


Figure 14. Sample Risk Map (Schmittling, 2010)

Business impact analysis. While risk assessment analyses the probability and impact of the risk and categorizes different risks across the organization, the purpose of business impact analysis is to give an idea of RTO and RPO by analyzing the impact of the risk. BIA includes risk assessment as a part of analysis.

Table 4

Differences between Business Impact Analysis and Risk Assessment

Risk Assessment	Business Impact Analysis
Output: The list of risks and their probability. Used for both information security and Business continuity	Output: Gives information on RTO and RPO Used only for Business continuity

Business impact analysis identifies how the identified risks may affect the business continuity and how quickly the processes should be recovered. Risk assessment is the

foundation for both DRP and BCP. Business continuity is all about impact on time sensitive functions and recovering those keeping time in mind. A bank can stop marketing when a disaster strikes, but it cannot stop working on transactions (Okolita, 2009). When people find themselves in stressful situations, these plans will guide them, and the best plans will always include checklists containing items and their priorities.

The next part after BIA would be to empower employees to tackle the situation and if the need more than just having workarounds on site, the business should set up duplicate systems in a secondary site. “The Business Continuity Plan should establish communications guidelines and service levels that will enable staff to effectively manage customer expectations throughout the disaster and its aftermath” (Pitney Bowes, n.d. p. 3). Organization has to settle on a choice based on their requirement of having systems and sites for business continuity.

Option for Acquiring Critical IT System.

Option	Expected Cost	Capability	Effort needed	Quality	Control	Desirability
As needed	High	Unknown	High	Low	Low	Low
Prearranged	Medium	Meets requirement	Medium	Medium	Medium	Medium
Reestablished	Low	Meets requirement	Low	High	High	Medium

Figure 15. Choices for Acquiring Critical IT Systems (Snedaker, 2007)

Option for Establishing Alternate IT Facilities

Option	Cost	Meets requirement	Effort	Quality	Control
Company cold site	Medium	Yes	Medium	Low	High
Hot site which is Outsourced	High	Yes	Low	High	Low

Figure 16. Choices for Establishing Alternate IT Facilities (Snedaker, 2007)

"The final part of the plan development is annual training. All persons involved, from the executives down through the on-site implementation team, must review the plan at least annually" (Pitney Bowes, n.d., p. 3). Most important aspect about this plan is that the plan should be verified under realistic conditions so that the plan works for a disaster most appropriately in the real scenario.

***Phase 2—Implementation*.** Once the plan is all set, disaster occurrence would not tense the situations as hardly as it would without a plan and crisis can be handled more tactfully by the organization.

Best practices to following during implementation phase:

- *Automate the BC plan*. At times, having just a BC plan that can run on manual resources is not enough. It would be illogical to have a good budget for a BC plan that can only run with human resources to recover from the crisis and hence it is time to automate at least some aspects of the plan (Tech Target, n.d.). Business continuity software is in the market from decades and has undergone many

changes. Now, with a business continuity software, BIA, incident management, testing, updating the plan, and checking for the accuracy of the plan with real time scenarios is very much possible. Having less human intervention indirectly means minimizing human error. Business continuity software, reduces time, improves efficiency and accuracy, meets already set standards, updates with new standards and changes (Milligan, 2016).

Figure 17. Coverage of Catalyst Business Continuity Software (Avaluation, 2017)

- Communication. Communication is very important when a disaster strikes. Organizations should make sure that there is no interruption in communication between the business continuity and disaster recovery team and the organization's staff on-site.

- Have a strategy to choose the secondary data center. The secondary data center is the place where the business continues to operate at the time of disaster. Organizations strategy for have a secondary data center will be done during the planning stage. Generally, any organization will have more than one secondary data center and sometimes the mission critical data is stored on cloud.
- Move. After having a strategy for secondary data center already planned, move to the new and secure location, only if the business is no more accessible from the primary location or if the situation might seem to get out of control.
- Employee safety. Employees are critical resources of an organization. Although, there are many business functions that are critical and that gets profits to the business, employees are the ones who maintain them both for safety and productivity. Hence, ensuring employee safety is not just an ethical and moral issue, but a very sensitive part of business continuity and disaster recovery plan.
- Securing information assets of clients. As discussed before in this paper, lack of business continuity plan and disaster recovery plan or evidences of improper implementation or poor documentation of BC and DR plans would lead to having legal issues and can additionally drag the company to court of justice and something worse than a disaster or crisis may happen. So, ensuring the security of information assets of the partner companies or clients will also be the primary goal of the BC plan or the DR plan.

- Accessible and consistent plan. In the event of disaster, most of the IT services might not work, physical equipment might get damaged and many other undesired things might happen. So, keeping the plan in a most accessible location so that employees need not search for it or must take a long painful path to reach the plan would help in critical times. Also, periodically improving the plan, adding new changes, reviewing and versioning the plan would also help in keeping the employees updated about BC and DR plan, also having the latest versions of the plan is always beneficial.
- Notify customers. Notifying customers and updating them about the success and working of the plan. Instead of hiding the truth from customers which will be known in any other way, notifying customers will instill confidence in them and will make regular customers, more loyal to the organization.
- Murphy's law. According to Murphy's law–if something should go wrong, it will go wrong. Disaster itself is, in many cases most unexpected but even with a proper disaster recovery or the business continuity plan, it is very common that some of the critical functions are still carried away by the disaster. So, make efforts to test the plan in different scenarios and most worst scenarios i.e. "expect the unexpected in the unexpected." This is the scenario where plan B comes into picture i.e. having a link up with a company that masters in disaster recovery or business continuity. Also, having a sub contingency plan for the actual contingency plan.

- Restore the services. Implement the plan structurally, also follow your instinct when necessary.

Figure 18. Disaster Response and Recovery Lifecycle for Business Continuity (Whiting Risk Consulting, 2017)

***Phase 3—Follow Up*.** It is essential to keep up momentum for the full-term of the recovery process, once plan starts to work and client needs are met (Pitney Bowes, n.d.). The main goal of business continuity and disaster recovery team is to get out of the crisis successfully but, it is not sufficient for a business to just pass the disaster with minimum damage. Disasters, many times, last for a longer period than expected, so it is very important for BC and DR team to be vigilant for certain period till the business is strong enough to tackle one more disaster. Japan is one of the best examples for this. Japan has seen three major disasters—nuclear disaster, earthquake, and tsunami—one after the other in a sequence. At

this point of time, the businesses are still fragile and cannot take the upcoming threats. A very good and fully functional business continuity plan will also include post-occasion projects.

Right decision on site recovery. Business must have an appropriate plan to decide when to replace and when to rebuild. If the recovery operations are ongoing in the primary location, then the staff and business operations should be moved to a secondary site. BC and DR staff must know when to replace and when to rebuild the physical plant (Pitney Bowes, n.d.).

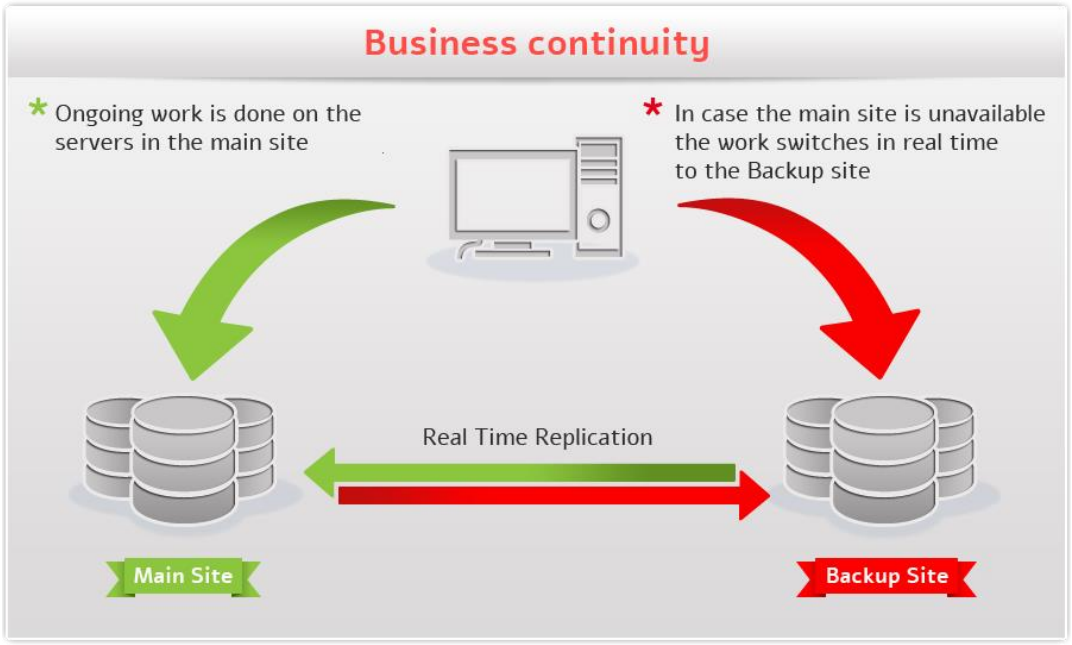


Figure 19. Backup Site for Business Continuity (BCP-DRP-VEEAM Solutions, n.d.)

Communication with employees and customers. After recovery and follow up, processes should also be communicated with the customers and employees to maintain confidence, trust and relationship with the stakeholders. Customers will have all the legal rights to know about the recovery process and the updates. If everything is rightly communicated, the feeling of being vulnerable and the confidence in returning to normalcy is gained.

Claim insurance. Insurance can help the business to be out of bankruptcy. Hence, keeping all the records of damages and repairs done.

Review of the incident. Conduct reviews for the incident to document the findings, loop holes in the existing plan, lessons learned, mistakes made etc. Later create a new version of the plan to add new procedures to tackle the situations that are out of scope during the current crisis. In this way, the plan makers will have a clear idea of what aspects of plan can be replicated in real time and what are merely an assumption of success.

Finally, be vigilant and be ready for the next disaster to be more successful in business continuity and recovery process.

Table 5

Most Effective Business Continuity Plan

Phase	**Project foundation**	**Business assessment**	**Strategy selection**	**Plan development**	**Implement test, assess, maintain**
Functions	Aligns management and eliminating resistance later in the project	Identifies both external and internal threat information found in this phase will be the basis for the recovery stage and the BCP plan	Employs recovery to eliminate conditions that would impact operation.	Puts to gather a sequence of actions to mitigate the identified threats and risk recoverability of key service.	Implements the BCP ensures that the BCP against published standards and keep it current.
Steps	1. Purpose, objectives, scope and assumptions 2. Plan coordinator and development team 3. Project plan	1. Perform the Threat analysis 2. Perform Business impact analysis	Strategy identification and strategy selection	Document business continuity plan	Implementation and testing of the plan by trained professionals

(Barnes, 2004)

A note on best practices for business continuity and disaster recovery plan. Following are some of the most important best practices to be followed while creating or deploying a business continuity and disaster recovery plan.

- Identify the key business processes.
- Identify the assets that keep the business processes running.
- Identify the processes to maintain the continuity.
- Consider the risks on different departments of the organization.

- Communication between the department needs to be standardized.
- BIA or RA, any of the process can go first but technically RA sets the basement for BIA and hence as a best practice RA should be conducted prior to BIA.
- Roles and responsibilities should be assigned to the personnel based on their departments, experience and involvement in the planning process.
- Standardize crisis communication both externally and internally.
- Keep a track of historical crisis, risks, failures and achievements.
- Track, report, redo each of the sub processes in the plan individually.

The following table contains business continuity or disaster recovery i.e. BC/DR standards and best practices given by different organizations that are accepted internationally. BC and DR standards vary based on the geographical location of the enterprise like the country where it is working in, based on the mission, vision and goals of the organization like banking, brokerage, healthcare, IT etc. The following standards will lay a strong foundation in building a better BC and DR strategy having the greatest power to resist a disaster. Saying this, there is no all-in-one plan for each and every disaster that may occur in future. Organizations must build a plan every scenario as each one needs different set of resources, budget, capacity, strength, strategy. There is no one stop solution for the selection of standards either as ISO 24762 provides the guidelines to select DR service provider (Kirvan, 2015), the importance of selecting a good DR service provider will be given in more detail, further in cloud-based disaster recovery.

Table 6

Standards that Address Business Continuity, Disaster Recovery, and Crisis Management Best Practices (Kirvan, 2015)

Standards	Topics Addressed	Organization Link
ISO 22300:2012	Societal Security – Vocabulary	www.iso.org
ISO 22301:2012	Business Continuity Management Systems – Requirements	www.iso.org
ISO 22311:2012	Video Surveillance	www.iso.org
ISO 22313:2012	Business Continuity Management Systems – Guidance	www.iso.org
ISO 22315:2014	Mass Evacuation – Guidelines	www.iso.org
ISO 22320:2011	Emergency management – Requirements for Incident Response	www.iso.org
ISO 22322:2015	Emergency management – Guidelines for Public Warning	www.iso.org
ISO 22324:2015	Emergency management – Guidelines for Color-coded Alert	www.iso.org
ISO 22351:2015	Emergency management – Message Structure for Interoperability	www.iso.org
ISO 22397:2014	Guidelines for Establishing Partnering Arrangements	www.iso.org
ISO 22398:2013	Guidelines for Exercises	www.iso.org
ISO 22399:2007	Guidelines for Incident Preparedness and Operational Continuity Management	www.iso.org
ISO 27031:2011	Guidelines for Information and Communications Technology Readiness for Business Continuity	www.iso.org
ISO 27031:2011	Guidelines for Information and Communications Technology Readiness for Business Continuity	www.iso.org
ISO 24762:2008	Guidelines for Information and Communications Technology Disaster Recovery Services	www.iso.org
ISO 27000	ISO Information Security Standard	www.iso.org
ISO 31000	ISO Risk Management Standard	www.iso.org

Table 6 Continued

Standards	Topics Addressed	Organization Link
BS 65000:2014	Organizational Resilience Standard	www.bsigroup.com
PAS 7000	Supply Chain Risk Management	www.bsigroup.com
BCI GPG 2013	Good Practice Guidelines from the Business Continuity Institute	www.thebci.org
BS 11200:2014	Crisis Management Standard	www.bsigroup.com
PD 25888	Guidance on Business Recovery	www.bsigroup.com
PD 25666:2010	Exercising BCM	www.bsigroup.com
PD 25111:2010	Human Aspects of Business Continuity	www.bsigroup.com
PD 25222	Guidance on Supply Chain Continuity	www.bsigroup.com
NFPA 1600:2013	American National Standard for business continuity and emergency management; approved as part of P.L.110-53 Private Sector Preparedness (PS-Prep) Act of 2009	www.nfpa.org
ASIS SPC.1:2009	Organizational Resilience Standard; approved as part of P.L.110-53 Private Sector Preparedness (PS-Prep) Act of 2009	www.asisonline.org
FFIEC BC Handbook	Business Continuity Planning; IT Examination Handbook (2008)	www.ffiec.gov
ISACA Document G32	IT Auditing Guideline; Business Continuity Plans	www.isaca.org
FINRA Rule 4370	Business Continuity Plans and Emergency Contact Information; consolidates NYSE Rule 446 and NASD Rules 3510 and 3520	www.finra.org
FEMA FCD	Federal Continuity Directives for government agencies	www.fema.gov
DRJ GAP	Disaster Recovery Journal Generally Accepted Practices	www.drj.com
NIST SP 800-34	Contingency Planning Guide for Information Technology Systems	www.nist.gov
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems	www.nist.gov
NIST SP 800-84	Guide to Test, Training and Exercise Programs for IT Plans	www.nist.gov

(Kirvan, 2015)

Research Question 3. *What are the different approaches taken by the organization's contingency plan to avoid risks on-site and on cloud?* In past few years, many companies have

moved from on-premise solutions to the hosted solutions i.e., cloud computing is embraced by many companies in past few years. With new technology, comes new hurdles and new risks. Although cloud computing gives an edge to data storage and a number of hosted services, provides broader scope for innovation and business transformation, many companies are still in dilemma to completely on-board their solutions on to the cloud. This is because of the risks and vulnerabilities associated with cloud. Cloud computing is viewed as serious security and compliance concern by some companies. But there is truly no correct perception about having or not having cloud based solutions. In fact, every arrangement requires a tradeoff between security, optimization and expenses. In the view of a company, cloud computing is security concern and security is the first inhibition to adopt cloud. Firewalls, anti-virus software, intrusion detection systems are relatively straight forward but securing the data and the applications on cloud that has no edge or perimeter is complex. With cloud computing, every corner has an unknown threat hiding and ready to attack and hence, business continuity and disaster recovery plans in cloud are equally and most important to protect the organizations data and to have continuity in the business.

Risks associated with cloud. Risks associated with cloud and how to reduce them:

1. With cloud computing and multi cloud environment it is difficult to know who is accessing which resources on which cloud. It is important for the company to have strict control over access privileges given to their employees, particularly when using cloud based services as it is relatively new and relatively more vulnerable.

2. Accessing data based on context is one way to reduce the risk of users using the data in unauthorized way. Users must be given access to data based on their geographical location and the way they are trying to access the data. Based on certain conditions, additional steps to sign in must be placed and limited access to certain resources must be provided.
3. Every organization has some set of data that is sensitive and losing such information be devastating. Additional mechanisms to protect such data should be considered like having the data encrypted or continuous monitoring of the data.
4. Mobile applications might have several vulnerabilities, and when using corporate data on mobile devices, it should be isolated from personal data.
5. Finally, provide a way to capture the audit logs to provide real time visibility for cloud infrastructure. Audit logs are basically used to see through the security risks and potential threats that breaches vulnerabilities in the existing system.

***DR challenges that can be resolved using cloud*.** Disaster recovery and business continuity can be viewed as business processes and every business process has its own challenges. Following are the challenges when planning for business continuity or disaster recovery.

Cost. Cloud has always been a best choice when it is the matter of cost. So is the case with cloud-based disaster recovery strategies. Usually, as the recovery time objective is decreased, the cost of recovery increases but when cloud based services are used for disaster recovery, time and money are reduced and resources are effectively used.

Synchronization. During disaster recovery, the business operations are moved to a secondary site. There should be same environment on both the primary site and the secondary site for the success of the recovery process. But most often, this is not the case, there is often a mismatch between the primary and secondary site which can be reduced or completed vanished while using cloud-based disaster recovery services.

Scalability. Traditional disaster recovery procedures having a secondary site lack the flexibility. As the requirements, environments and demands of the technology and situations change, traditional disaster recovery techniques lack to accommodate so many changes and is costly. But, with cloud-based disaster recovery, scalability is not a concern. In fact, many companies choose an amazon web services unit and put a little portion to disaster recovery and then scale the resources as required during the time of crisis.

Difficulty in managing. Cloud-based disaster recovery is an easy to use solution for a disaster recovery process. Most of the tasks are automated, accurate and consistent which means speedy and painless recovery that costs less and is most accurate. Traditional disaster recovery strategies rely upon human intervention which leads to human error and slow process which in turn means lost revenue and sometimes lag in recovery process.

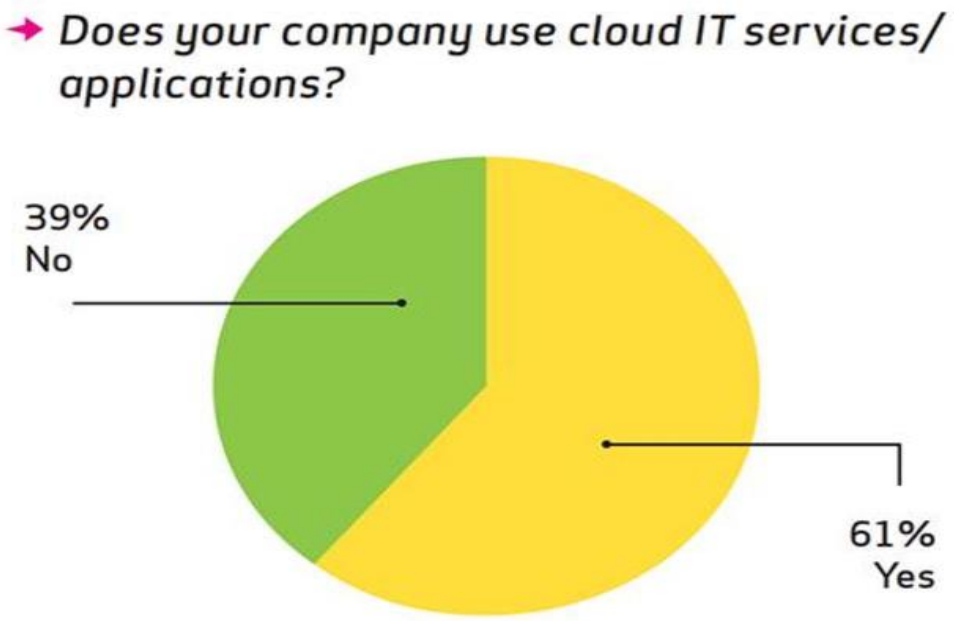


Figure 20. Percentage of Companies Using Cloud for IT Services (Pariseau, 2012)

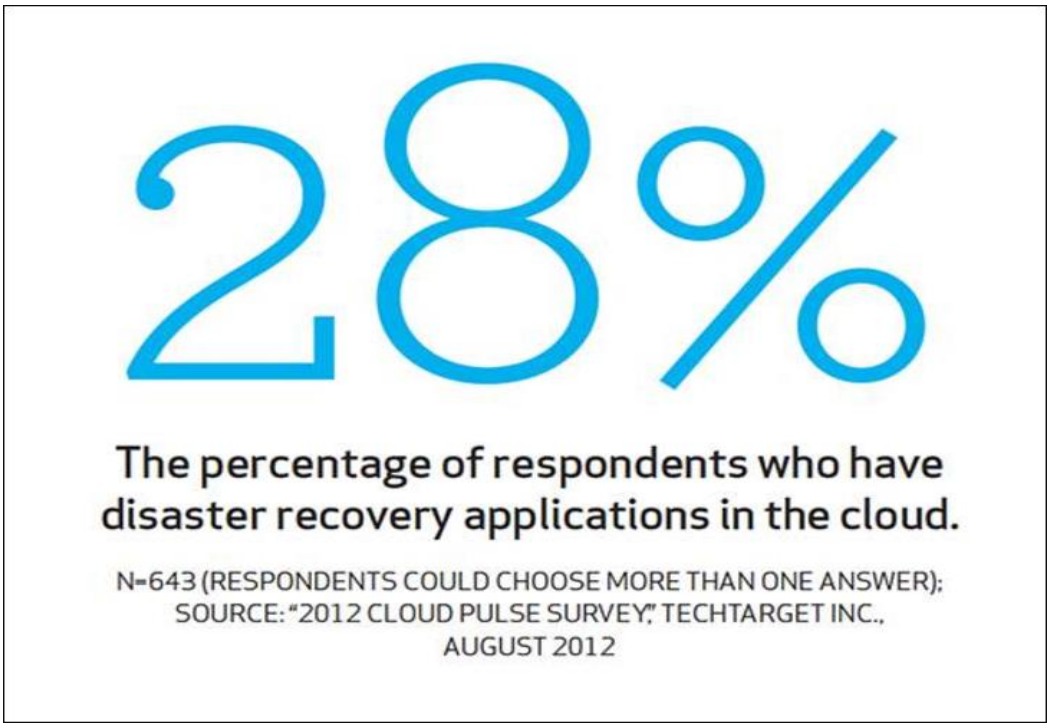


Figure 21. Percentage of Companies that Use Cloud-Based Disaster Recovery Services (Pariseau, 2012)

How to choose a cloud service provider for business continuity or disaster recovery.

- Downtime. The first consideration or factor to choose a cloud-based disaster recovery or business continuity service provider is the maximum allowable downtime. According to Spiteri, most clients expect the maximum allowable downtime to be 49 minutes on an average and 1 hour maximum (Spiteri, 2017). Downtime is the factor that decides if the disaster recovery strategy opted is a success or failure. Also, the downtime differs with the approach taken by the organization to use the disaster recovery services from the cloud provider like DRaaS or SaaS or BaaS or RaaS.

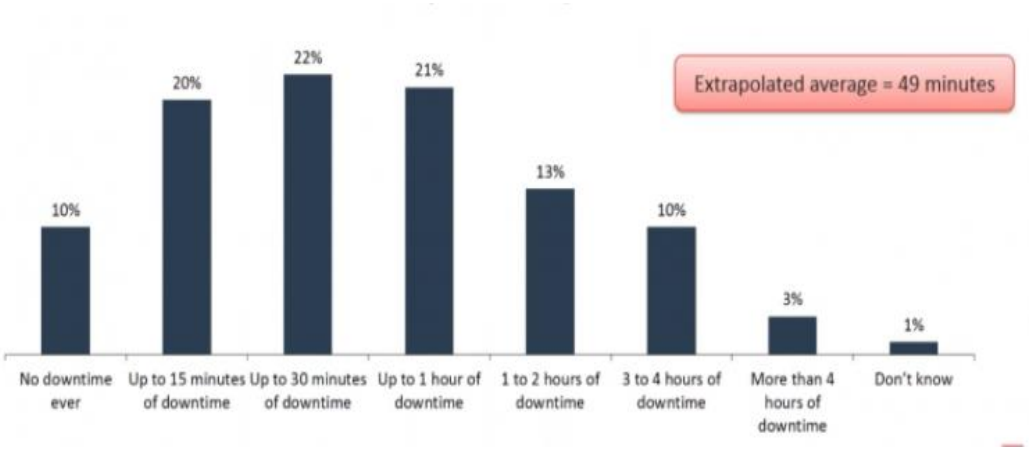


Figure 22. Maximum Allowable Downtime as Given by 280 Respondents (Spiteri, 2017)

Figure 22 is the bar chart deduced from a survey conducted on 280 respondents to understand the maximum accepted downtime in their organizations with the cloud-based disaster recovery service they use.

- Services provided. Many cloud-based disaster recovery service providers are merely backup service providers and not the actual disaster recovery service providers.

Although, backup is also a part of disaster recovery, but disaster recovery is much more than just a data backup service. As mentioned in the previous sections, there are different kinds of services provided by different service providers like storage as service (SaaS), backup as service (BaaS), replication as service (RaaS) and finally disaster recovery as service (DraaS). These services are just the high-level idea of the final output that an organization will get because of their choice of service and service provider. So, enterprise must dig deep into the list of services provided as part of either SaaS or DraaS or RaaS or BaaS like monitoring, maintenance services.

- Expertise. Expertise of the business continuity and disaster recovery service providers, on cloud, BC and DR is very important. Most of the time, organizations do not have a BC and DR team on their own, they depend on the third-party service providers. So, it is very critical that the third-party service providers have good amount of knowledge to provide insights into the BC and DR to the company and staff. It is their expertise that matters as the organization must fully believe that the third party can successfully complete the disaster recovery and continue business with minimal to no losses.
- Service providers that are in market for a long time. It is general human tendency to believe the people that are in market for long. It is obvious that they have good knowledge and command over the services they are providing from a long time and the reputation they earned by the services they provided. Although this is true in many cases, but this factor comes in the bottom when choosing a cloud service

provider because there are many service providers that have been in business from many years but are only working on backup services and there are some new service providers in the market that have very good disaster recovery services at their hand. At times, the longevity of service providers counts, and this has to be the last consideration for choosing a service provider.

Following are the approaches taken by the organization's BC and DR plan for Business continuity with cloud:

1. Build resiliency in the application itself. For example, Decide.com that uses amazon web services for the hosted cloud service, uses build in software code to fail gracefully. "When Amazon.com had an outage in June, e-commerce website Decide.com barely felt any impact "because we're geographically distributed, and we're set up to handle issues if it's not across all of Amazon" (Pariseau, 2012, ¶6).
2. Cross-Cloud Resiliency. Having the cloud app tied to one single cloud will not help. Cross cloud resiliency is using multiple clouds to provide resiliency to the web applications. This is possible, but it is again a tradeoff between security and expenses.
3. Built-in cloud resiliency. Some industry observers believe that built-in cloud resiliency will become a tool in the business continuity and disaster recovery (BC/DR) toolbox but will not take the place of today's familiar DR procedures (Pariseau, 2012). "Data deduplication, controller multi-tenancy, and fast site-to-site

replication make cloud storage systems a powerful part of the DR process" (Kleyman, 2014, ¶7).

Cloud-based disaster recovery services are the best as they are cheaper than having secondary infrastructure and a site to have all the IT infrastructure that are most of the time idle. With cloud, very limited infrastructure can be chosen and paid for and when the time comes for disaster recovery the IT resources can be scaled as per the requirement to recover from the disaster. As the cloud services are usage based, company will only pay for those limited resources till there is any need for extra IT infrastructure. Cloud-based disaster recovery sites leads to cost reductions as there is no need to have a secondary data center with all the infrastructure in it.

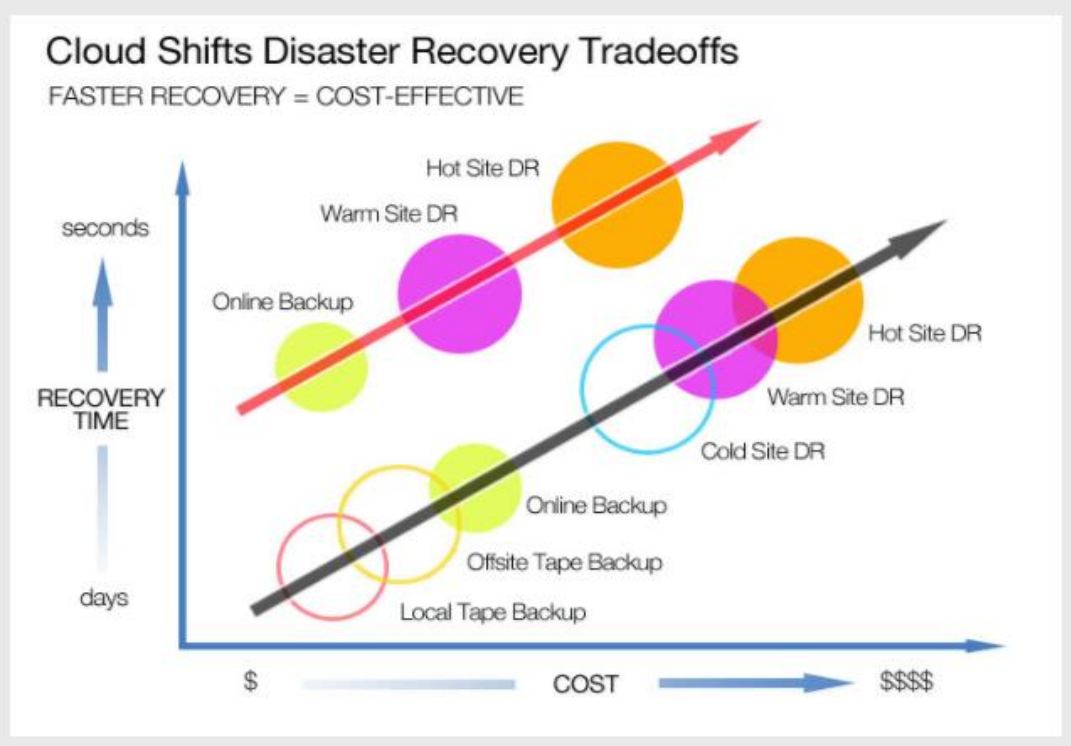


Figure 23. Reduced Recovery Time with Cloud-Based Recovery (Online Tech, 2016)

The approach to create a cloud-based disaster recovery plan is same as with the traditional disaster recovery plan. The first step would be to prioritize the resources based on their importance and criticality of the situation if that resource is unavailable for the business. Recovery time objective (RTO) and recovery point objective (RPO) should be determined. “The more focused a DR plan is, the more likely you’ll be able to test it periodically and execute it within the defined objectives” (Gsoedl, 2011, ¶9).

Cloud-based DR approaches side-by-side

	Managed primary and DR instances	Cloud-based backup and restore	Replication in the cloud
Instances	• Salesforce.com CRM • Email in the cloud	• On-premises into the cloud • Cloud to cloud	• On-premises into the cloud • Cloud to cloud
Merits	• Fully managed DR • 100% usage based • Least complex	• Only requires cloud storage; cloud virtual machines are optional • Usually less complex than replication	• Best recovery time objectives (RTOs) and recovery point objectives (RPOs) • More likely to support application-consistent recovery
Caution	Service-level agreements define access to production and DR instances	Less favorable RTOs and RPOs than replication	Higher degree of complexity
Implemented via . . .	N/A	Backup applications and appliances	• Replication software • Cloud gateways • Cloud storage software such as EMC Atmos and Hitachi HCP

Figure 24. Approaches for Cloud-Based Disaster Recovery (Gsoedl, 2011)

Figure 25 shows the flow chart that describes how to choose a cloud backup service based on the business need. According to the figure, there are four different kinds of services that cloud provides, disaster recovery as service (DRaaS), Storage as service (SaaS), Backup as service (BaaS), and Replication as service (RaaS).

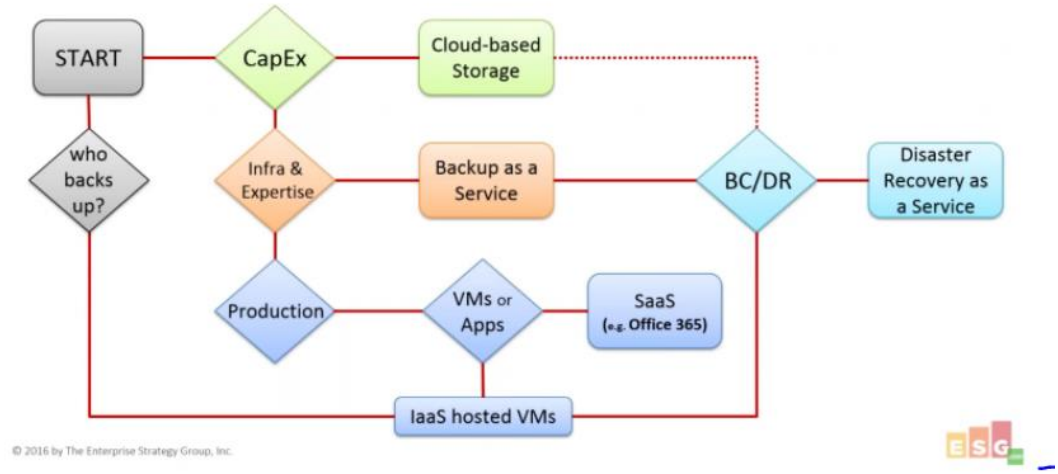


Figure 25. How to Choose Service Provider (Spiteri, 2017)

Following are some approaches to choosing a service provider:

- Approach 1. This is the case of pure cloud based IT services where both the primary and DR instances are incorporated into the cloud. With this approach, an organization can get 100% benefit of using cloud based service, but it is very important to have a defined service level agreement (SLA) to make sure that delivery of services is uninterrupted for both primary instance as well as disaster instance. At this point, choice of the service provider makes a huge difference. If the service provider chosen by the business is incorrect, it will lead to many complications in the serving the business process. But with a good service provider like Amazon and a

defined service level agreement (SLA) the business can function smoothly with the lowest bid cost on those services.

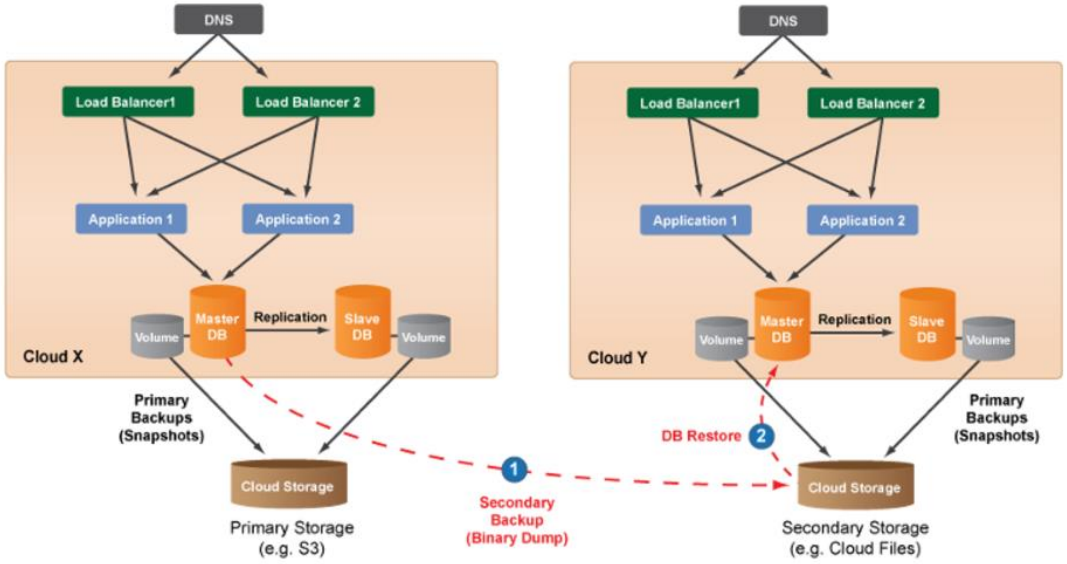


Figure 26. Managed Primary and DR instances (Rignt Scale Docs, n.d.)

- Approach 2. In the second approach, enterprise is not completely dependent on cloud for all its IT services. Cloud is used for backup and recovery while applications remain on premise. During the disaster having a backup is very important, it induces confidence in the organization's stake holders that their information is safe even after the disaster. Cloud backups are relatively easy compared to recovery. There are many vendors that take care of data back up and synchronization into the cloud, but the challenge is to recover the data back into the on-premise hardware meeting the RTO. If this approach is chosen by the organization then it would be recommended to have a local back up and a cloud back up where cloud back up is the secondary back up to be on a safe side.

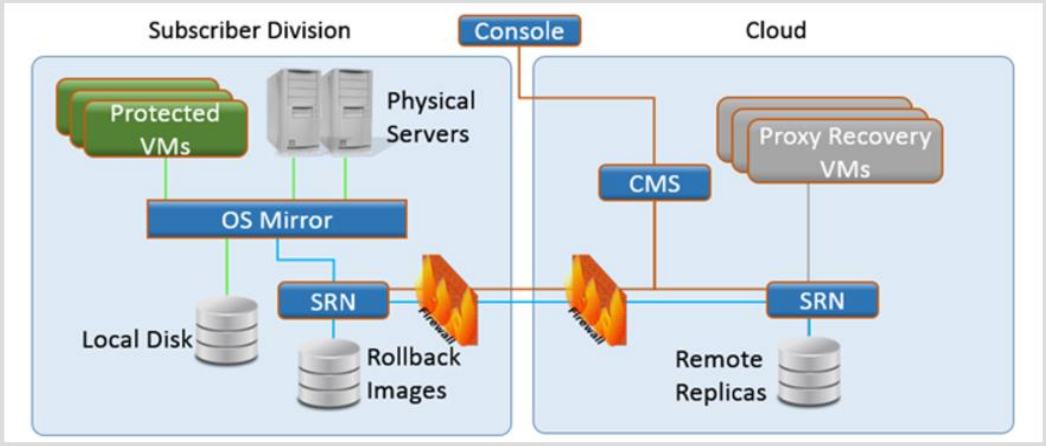


Figure 27. Cloud-Based Backup and Restore (Century Link Cloud Blog, 2014)

- Approach 3**.** In this approach, data is replicated from on-premise to cloud virtual machines. Replication is done to protect the mission critical data such as production instances. Replication can be done from cloud virtual machines to cloud virtual machines or from on-premise to cloud-virtual machines. This approach is opted for business processes where RTO and RPOs are very critical and should have the minimum value possible. “Replication products are based on continuous data protection (CDP), such as CommVault Continuous Data Replicator, snapshots or object-based cloud storage such as EMC Atmos or the Hitachi Content Platform (HCP)” (Gsoedl, 2011, ¶21).

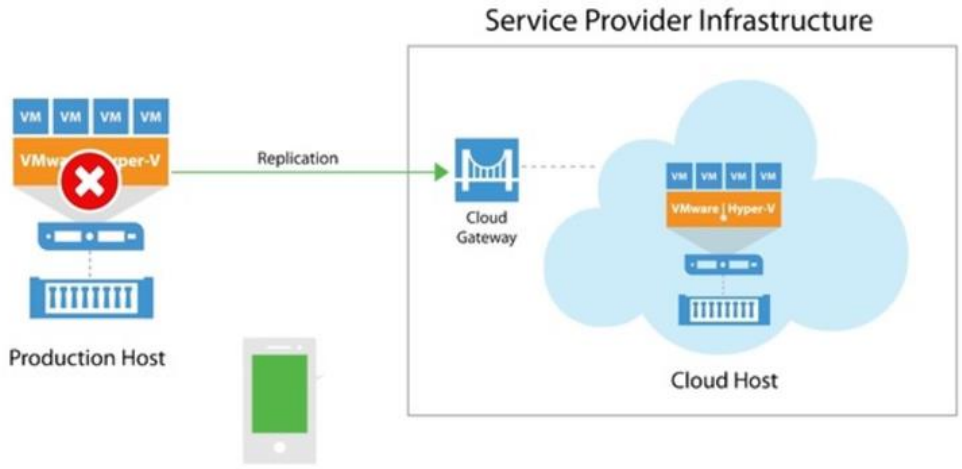


Figure 28. Replication into the Cloud (Veeam, n.d.).

While a cloud-based approach is most appealing for any enterprise, as there are many benefits associated with it, like the service can be implemented without the need to purchase infrastructure, maintain and have personnel to support it, paying only for what is used, adding additional capacity as much as required by the organization. In fact, having a public cloud as the BC/DR solution is the cheapest and effective solution. There are many important issues to be considered before making a choice of the kind of cloud service an organization want to use and from which service provider. Most of the DRaaS simply provide cloud-based backups and not recovery options. Hence, organizations should consider the following features provided by their service provider:

1. Data backups, replication, failover, failbacks are most complex, time taking and expensive. Automation can make the process a lot more easier and more accurate and consistent while testing, deploying and recovering the original data. Disaster

recovery service providers should have automation as one of the key features in the services they provide.

2. More human involvement directly means more human error and lot of complexities, dependencies. With cloud-based approach, minimal human effort is required whether it is on-premise recovery or on cloud recovery and certainly zero human error. Organizations have to look for a unified infrastructure for the management of the workloads.
3. With legacy approach, testing is very rarely done and even if the disaster recovery and business continuity plans are tested for success and failure cases, there is no guarantee that these tests would be a success in real. If an organization is opting for cloud-based approach, automation of testing of a set of workloads and full recovery should be one of the services that the disaster recovery service provider should provide. Cloud-based disaster is undoubtedly cheap, but only if a good service provider is chosen.
4. Until the business can run on-premise, all the critical processes should be able to recover and run in cloud. There should not be any constraint on how long the processes will run on cloud, so that even if the recovery on-premise is slow, business will still run in cloud without having the fear of performing a fast cloud to on-premise.

For companies to shift to a disaster recovery as service provided by cloud service providers is extremely difficult as it requires company to have full faith on the service provider

and there should be a good fit solution. At the end, disaster recovery and business continuity are what matters to the organization.

Success and Failure Stories of Some Companies

The Fukushima nuclear power plant, which is owned by Tokyo Electric Power (Tepco), can stand in the first place in the list of disasters in business continuity. Tepco was reported to have 15 billion losses in its account and was forecasted to be out of business in just few years. Tepco's business continuity plan was only designed for tsunami and not nuclear power plant failure and hence the company could not continue the business anymore after the nuclear failure although, it could survive tsunami.

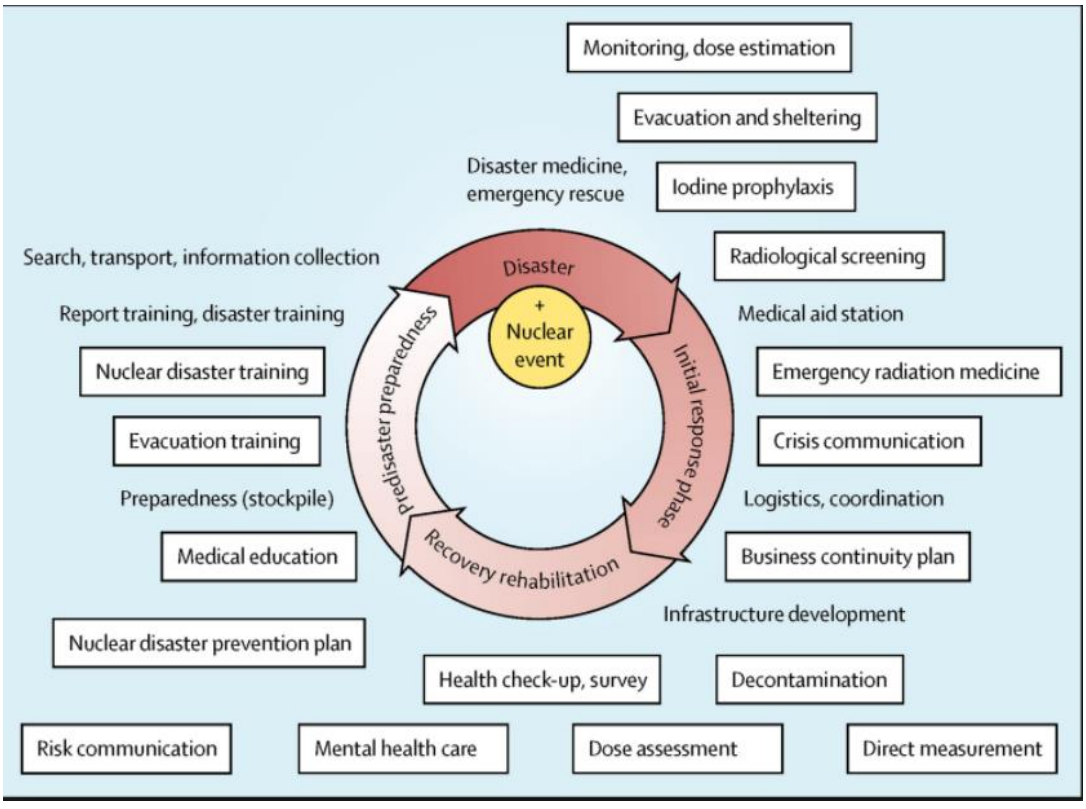


Figure 29. Lessons Learned from Fukushima Nuclear Power Failure (Ohtsuru, Tanigawa, & Kumagai, 2015)

An IT company, Cantey Technology has a success story with its business continuity plan. Cantey is a company that hosts servers for around 200 clients. There was fire in Cantey due to lightening which resulted in destruction of all the equipment present in every corner of the company. There was no scope to repair the infrastructure as every part was destroyed. Even after all the destruction, the clients did not feel even a pinch of pain, all thanks to the business continuity plan of the company. Backups were taken continuously, servers were moved to remote data center and staff to secondary location.

Northern Lincolnshire—everyone in UK might know this name. Northern Lincolnshire and NHS foundation trust are a chain of hospitals. In November 2016, this chain of hospitals was infected with a virus and in a matter of five days—three hospitals were infected, and the systems were not working. Patients were not attended, and even major cases were turned down. The reason for the downtime was literally not expected from this network of hospitals—and not from a hospital in the first place. There was no business continuity plan in place for any kind of disaster with Northern Lincolnshire or NHS foundation trust.

Hurricane Irma and Hurricane Harvey are the recent examples of how a business continuity and disaster recovery plans of the organizations may fail and how weak plans can be identified. It is always better for the organization to test, retest, and retest the plans for all the scenarios.

Above are some examples of how can a good disaster recovery and business continuity plan save the organization and how bad or no business continuity or disaster recovery plan can bring the organization huge losses.

Summary

This chapter presents the results of the qualitative research on the topic “Business Continuity and Disaster Recovery Plan for Information Security. This chapter will provide the results of three questions to be addressed as a part of the research i.e. how can an organization make their plan sustainable, best practices to plan, build and implement a disaster recovery and a business continuity plan on cloud. This chapter will also provide a list of organizations that provided the standards for different aspects of crisis management, risk management, disaster recovery and business continuity.

Chapter V: Conclusions and Future work

Introduction

Learning is a never-ending process. As new technologies come in, there comes scope for new inventions in certain topic like the standard, traditional approach in developing a business continuity and disaster recovery plan have shifter to having a cloud-based disaster recovery and business continuity approach. This chapter will provide the conclusion and the summary of this research paper. Future work that can be done after this research will also be discussed in this chapter.

Conclusions

Business continuity and disaster recovery plans play a very key role in an organization's sustainability in this competitive business world. BC and DR plans are like audit logs, although they have no importance or share in profit generation and in fact an additional overhead to daily work activities, they indeed help in sustaining through tough situations. In this paper, disaster recovery and risk management are considered to a part of business continuity, as a part of business continuity operations are completed if risk management and disaster recovery are completed successfully. There are many different organizations that provide standards to design, develop, and deploy business continuity and disaster recovery plans and an organization has to keep a strict eye on their requirement and standards that their plans have to meet. In general, one plan for every disaster will never work. Companies must build a plan for each disaster or each set of commonly co-occurring disasters. Using cloud-based disaster recovery services will help get the most out of cloud based services while having to spend very

less on the plans than opting for a traditional approach but companies must consider the service provider agreements, SLA's otherwise cloud based services will be no less than overhead to company. In few words, disaster recovery and business continuity plans are no more an accessory, businesses are unknowingly in a dire need of that helping hand at the time of disaster which we call BC and DR Plan and for the organizations to sustain, they must plan, design, deploy and maintain these plans.

Future Work

This research paper has not discussed much about the automation of business continuity and disaster recovery plan. Although the topic was addressed as a part of making the BC and DR plan more sustainable, it can be given more scope to research. While cloud-based disaster recovery service is understandable, business continuity with cloud can be a topic that can be researched in depth. So, the future work for this research paper can contain automation of business continuity and a disaster recovery plan and having cloud-based business continuity services.

Automation of business continuity and a disaster recovery plan will give many benefits for the company in terms of budget, consistency, meeting standards, updating the software, testing, updating the plan according to the latest technology changes, maintenance, and using the business continuity software will lead to having a standard format throughout the organization. Many modules that contribute to different aspects of a business continuity plan like business impact analysis, incident management, emergency notifications can be created and integrated if business continuity software is used. From time to time, many changes occur

in the organizational structure and facilities and these kinds of changes are easily accommodated by automating the BD or DR plan. These are some of the examples of the benefits of automation of BC and DR plan which can be researched in detail and can deduce different factors in the BC or DR software that are to be considered by the organization before a BC or DR software is purchased. Also, an in-detail research on the software currently available in the market to perform the automation of BC or DR plan can be done as part of the extension to this paper. The following figure can give a brief idea on which business continuity software to consider for the research. The figure is the result of Gartner research—Gartner is a registered trademark and provides high quality research on different vendors in the market related to concept of research (Strategic BCP, 2017). As shown in Figure 30, the top 10 business continuity management software are:

- Fusion Risk Management
- Strategic BCP Resilience ONE
- Avaluation
- Sungard Availability Services
- Recovery Planner
- Lockpath
- Clearview
- Continuity Logic
- Dell Technologies
- Metric Stream

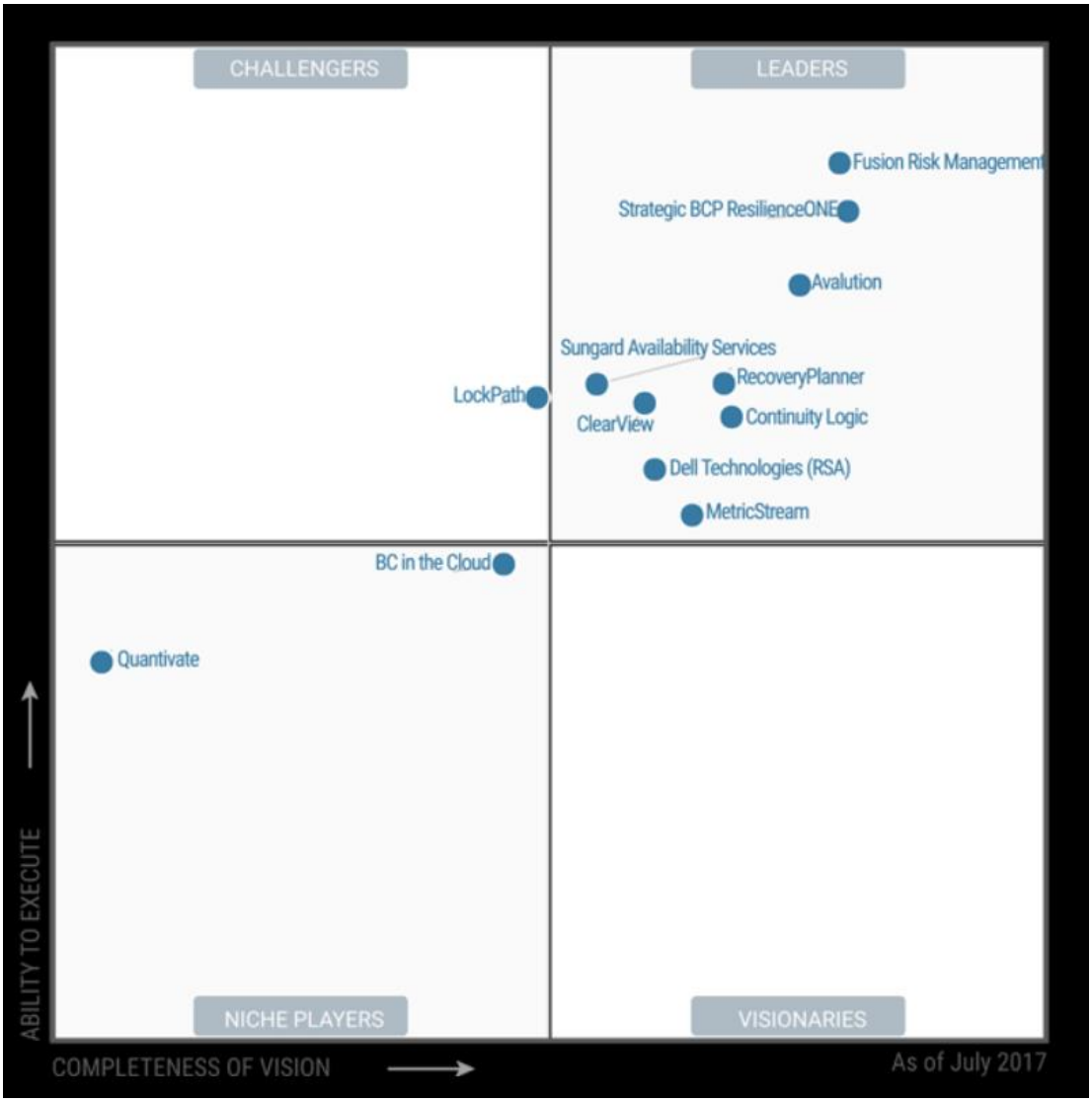


Figure 30: Leaders in Business Continuity Management Software (Gartner Magic Quadrant for Business Continuity Management Program Solutions, 2017)

Secondly, business continuity services on cloud can be taken as a research topic. BC as a cloud service is a relatively new topic, although there are many cloud service providers that provide disaster recovery and back-up services, cloud-based business continuity service is relatively new. During the disaster, recovering from the disaster that has already happened is the first concern and continuing the business while performing disaster recovery is the second

important aspect. So, when a disaster occurs in a physical location, recovering and continuing business using cloud services is one of the best options that an organization can choose as cloud has many benefits as discussed earlier in this paper.

References

Avaluation. (2017). *Business continuity software*. Retrieved from http://www.avalution.com/business-continuity-software

Barbara, M. (2006). *Determining the critical factors of an effective business continuity or disaster recovery program in a post 9/11 world: A multi-method approach*. Retrieved from http://spectrum.library.concordia.ca/9033/1/MR20809.pdf

Barnes, J. C. (2004). *Business continuity management in health care environment.* Brookfield, CT: Rothstein Assoicates Inc.

BCP-DRP-VEEAM Solutions. (n.d.). *Tower watch solutions LTD*. Retrieved from http://www.towerwatchtech.com/pcbdrp/

Bejtlich, R. (2004). *The tao of network security monitoring: Beyond intrusion detection.* Boston, MA: Addison-Wesley Professional .

Berman, A. (2015). *Risk management and business continuity: Improving business resiliency*. Retrieved from http://www.riskmanagementmonitor.com/risk-management-and-business-continuity-improving-business-resiliency/

Britton, C. (2016). *Risks and vosts of not having a business continuity management program*. Retrieved from https://www.rockdovesolutions.com/blog/risk-costs-of-not-having-a-business-continuity-management-program

Century Link Cloud Blog. (2014, December 8). *DataGardens joins CenturyLink, adding proven disaster recovery offering to cloud portfolio*. Retrieved from https://www.ctl.io/blog/post/datagardens-joins-centurylink-adding-proven-disaster-recovery-offering-to-c/

Disaster Recovery. (n.d.). *Evaluating and applying relevant BCM standards*. Retrieved from https://www.drj.com/642-a-bcm-professional-s-playbook-on-evaluating-and-applying-relevant-bcm-standards/file.html

Economist. (2011). *Costliest natural disasters till date*. Retrieved from http://www.economist.com/blogs/dailychart/2011/03/natural_disasters

Edwards, B. (1994). Developing a successful network disaster recovery plan. *Information Management and Computer Security, 2*(3), 37-42. doi:10.1108/09685229410066200

Gregg, M. (2009). Business continuity and disaster recovery planning. *Pearson IT Certification*. Retrieved from http://www.pearsonitcertification.com/articles/article.aspx?p=1329710&seqNum=3%20Gregory,%20P.%20H.%20(2008)

Gsoedl, J. (2011). Disaster recovery in the cloud explained. *Tech Target*. Retrieved from http://searchdisasterrecovery.techtarget.com/feature/Disaster-recovery-in-the-cloud-explained

Hanning, S. (2001). Recovering from disaster: Implementing disaster recovery plans following terrorism. *SANS Institute*. Retrieved from https://www.sans.org/reading-room/whitepapers/recovery/recovering-disaster-implementing-disaster-recovery-plans-terrorism-558

Harwood, M. (2015). *Internet security: How to defend against attackers on the web* (2nd ed.). Burlington, MA: Jones and Bartlett Learning.

Heng, G. M. (1996). Developing a suitable business continuity planning methodology. *Information Management and Computer Science, 4*(2), 11-13. doi:10.1108/09685229610121008

Janco Associates. (n.d.). *Disaster recovery/business continuity and security template bundle*. Retrieved from https://www.e-janco.com/drp_and_security.htm

Kahan, S. (2014). *Global benchmark study reveals 73% of companies are unprepared for disaster recovery*. Retrieved from http://drbenchmark.org/global-benchmark-study-reveals-73-of-companies-are-unprepared-for-disaster-recovery/

Kamath, J.-P. (2007). Disaster planning and business continuity after 9/11. *ComputerWeekly.com*. Retrieved from http://www.computerweekly.com/news/2240082860/Disaster-planning-and-business-continuity-after-9-11

Kirvan, P. (2015). Today's most popular business continuity/disaster recovery standards. *Tech Target*. Retrieved from http://searchdisasterrecovery.techtarget.com/tip/Todays-most-popular-business-continuity-disaster-recovery-standards

Kleyman, B. (2014). Combining cloud with disaster recovery and business continuity. *Data Centre Knowledge*. Retrieved from http://www.datacenterknowledge.com/archives/2014/10/20/combining-cloud-disaster-recovery-business-continuity

Lancaster, D. (2002). Systems survivability. *SANS Institute*. Retrieved from https://www.sans.org/reading-room/whitepapers/recovery/systems-survivability-560

Lucht, M. J. (2014). *Launching a sustainable business continuity program in a higher ed culture (without getting eaten alive).* Retrieved from https://www.educause.edu/sites/default/files/library/presentations/E14/SESS023/Educause%2B2014%2B-%2BLaunching%2Ba%2BSustainable%2BBC%2BProgram%2B-%2BCMU%2B-%2BFV.pdf

Marek, Z. (2013). *Business continuity/disaster recovery*. Retrieved from http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

Martin, B. C. (2002). *Disaster recovey plan: Strategies and process*. Boston, MA: SANS Institute.

Mearian, L. (2011). 9/11: Top lessons learned from disaster recovery. *ComputerWeekly.com*. Retrieved from http://www.computerworld.com/article/2510996/disaster-recovery/9-11--top-lessons-learned-for-disaster-recovery.html

Milligan, L. (2016). It's time to automate business continuity and disaster recovery. *Disaster Resource Guide*. Retrieved from http://www.disaster-resource.com/index.php?option=com_content&view=article&id=822

Ohtsuru, A., Tanigawa, K., & Kumagai, A. (2015). Nuclear disasters and health: Lessons learned, challenges, and proposals. *The Lancet, 386*(9992), 489-497. doi:S0140-6736(15)60994-1

Okolita, K. (2009). *How to perform a disaster recovery business impact analysis*. Retrieved from http://www.csoonline.com/article/2124593/emergency-preparedness/how-to-perform-a-disaster-recovery-business-impact-analysis.html

Online Tech. (2016). *Benefits of disaster recovery in cloud computing*. Retrieved from http://www.onlinetech.com/resources/references/benefits-of-disaster-recovery-in-cloud-computing

Pariseau, B. (2012). Business continuity moves to the cloud as applications become resilient. *Tech Target*. Retrieved from http://searchcloudcomputing.techtarget.com/feature/Business-continuity-moves-to-the-cloud-as-applications-become-resilient

Pitney Bowes. (n.d.). *Best practices in business continuity*. Retrieved from http://news.pb.com/white-papers/best-practices-in-business-continuity.download

Prleap. (2016). *Janco releases disaster recovery business continuity planning template which contains management guidelines focused on addressing ransomware*. Retrieved from http://www.prleap.com/pr/248398/janco-releases-disaster-recovery-business

Public Safety Canada. (2015). *Guide to business continuity planning*. Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/bsnss-cntnt-plnnng/index-en.aspx

Rignt Scale Docs. (n.d.). *Disaster recovery or cloud migration scenario*. Retrieved from http://docs.rightscale.com/cm/management_guide/disaster_recovery_or_cloud_migration_scenario.html

Rouse, M. (2015). Business Impact Analysis (BIA). *TechTarget*. Retrieved from http://searchstorage.techtarget.com/definition/business-impact-analysis

SANS Institute. (2002). *Introduction to business continuity planning.* Retrieved from https://www.sans.org/reading-room/whitepapers/recovery/introduction-business-continuity-planning-559

Schmittling, R. (2010). Performing a security risk assessment. *ISACA, 1*. Retrieved from https://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-security-risk-assessment1.aspx

Schwalbe, K. (2015). *Information technology project management.* Independency, KY: Cengage Learning.

Scofield, L., & Martinez, E. (2011). *Assessing firm organizational risk.* Retrieved from https://www.aicpastore.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2011/CorpFin/AssessingOrganizationalRisk.jsp

Snedaker, S. (2007). *Business continuity and disaster recovery for IT professionals.* Retrieved from http://www.flood.rmutt.ac.th/wp-content/uploads/filebase/Related%20articles%20and%20writings/Related%20articles%20and%20writings%20(Eng)/Disaster%20Management%20Eng/Business%20Continuity%20and%20Disaster%20Recovery%20Planning%20for%20IT%20Professionals.pd

Spiteri, A. (2017, March 6). How to choose a trusted cloud service provider. *Veeam*. Retrieved from https://www.veeam.com/blog/how-to-choose-cloud-service-provider.html

Strategic BCP. (2017). *Gartner magic quadrant for business continuity management program solutions*. Retrieved from http://www.strategicbcp.com/resources/gartner-magic-quadrant.php

Tech Target. (n.d.). *Symantec, best practices for business continuity*. Retrieved from https://www.symantec.com/content/en/us/enterprise/white_papers/b-techtarget-top-7-best-practices-for-business-continuity-WP.pdf

Telovations. (2012). *Breakdown: Disaster recovery and business continuity*. Retrieved from https://telovations.wordpress.com/tag/revenue-lost-due-to-natural-disaster/

Veeam. (n.d.). *Cloud-based disaster recovery and offsite backup*. Retrieved from https://www.veeam.com/cloud-connect.html)

Wheatman V v. (2001). *Aftermath: Disaster recovery*. Stamford, CT: Gartner Research, AV-14-5238.

Whiting Risk Consulting. (2017). *Disaster recovery*. Retrieved from http://www.whitingriskconsulting.com/services/

Widup, S. (2003). Business continuity planning in difficult economic times. *SANS Institute*. Retrieved from https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-difficult-economic-times-1114

Yang, C.-l., Yuan, B. J., & Huang, C.-Y. (2015). Key determinant derivations for information technology disaster recovery site selection by the multi-criterion decision making model. *Eurasia Journal of Mathematics, Science, and Teachnology, Education*, *13*(8), 4553-4589. doi:10.3390/su7056149