LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5052NI Risk, Crisis & Security Management

Assessment Weightage & Type

50% Individual Coursework

Year and Semester

2021-22 Autumn

Student Name: Aadarsha Muni Shakya

London Met ID: NP01NT4S210023

College ID: 20049438

Assignment Due Date: 3rd January 2022

Assignment Submission Date: 3rd January 2022

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.

Module Code:	**CC5052NI**
Module Title:	**Risk, Crisis and Security Management**
Module Leader:	**Mr. Saroj Lamichhane** (Islington College)

Coursework Type:	**Individual**
Coursework Weight:	This coursework accounts for **50%** of your total module grades.
Submission Date:	**Week 11**
When Coursework is given out:	**Week 5**
Submission Instructions:	Submit the following to College RTE department before the due date: ● **Report in PDF format**
Warning:	London Metropolitan University and Islington College takes Plagiarism seriously. Offenders will be dealt with sternly.

Acknowledgement

I am really grateful because the technical report on the topic Business Continuity Planning and Disaster Recovery Planning is completed. Also, it would have been impossible to complete this report without the help of the module leader Saroj Lamichhane and module teacher Sandesh Gurung. The resources provided by the teachers helped me in the overall report.

Table of Contents

Table of Figures

Abstract

In this report in-depth research on the topic Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) is done. It covers all the components of BCP and DRP like Contingency Planning and Business Impact Analysis are also covered. Also, many cases of organizations implementing proper BCP and DRP to avoid severe damage are also analysed. Not just proper but organizations who didn't implement BCP and DRP are also analysed.

1. Introduction

Business Continuity Plan (BCP) is the acts of finding disruptions, ensuring prevention or less chance of occurrences and responding to any such incident in a planned and rehearsed manner to recover the losses and bring the business back into operation.

Whereas Disaster Recovery Plan (DRP) focuses on resuming work after an unplanned incident in the primary site. It is applied to the aspects of an organization that depend on a providing service. DRP also aims to resolve the losses and restart its operations fast in a minimal level.

1.1 Aims

The aim of this report is to show the importance of implementing BCP and DRP in an organization. When a distortion occurs, those planning will help the organization to react accordingly.

1.2 Objectives

The objectives of establishing BCP and DRP in an organization are:

- To define BCP and DRP
- To determine the steps during and after a distortion
- To provide alternate ways to provide service

2. Background

First of all, in order to implement proper Business Continuity Plan and Disaster Recovery Plan a proper contingency planning is important. Contingency planning is a set of planes designed to help an organization's production and service in events or situations that may or may not occur (TechTargate, 2015).

While making a contingency plan, there are six steps to implement a proper contingency plan and they are identifying the needs, identifying the resources, anticipating disruptions, selecting strategies, implementing strategy, and testing and revising the plan.

A proper contingency plan includes Business Impact Analysis (BIA), Incident Response Planning (IRP), Disaster Recovery Planning (DRP), and Business Continuity Planning (BCP). This plan is designed to predict consequences, find possible impact, and react according to the disruption (MacNeil, 2021).

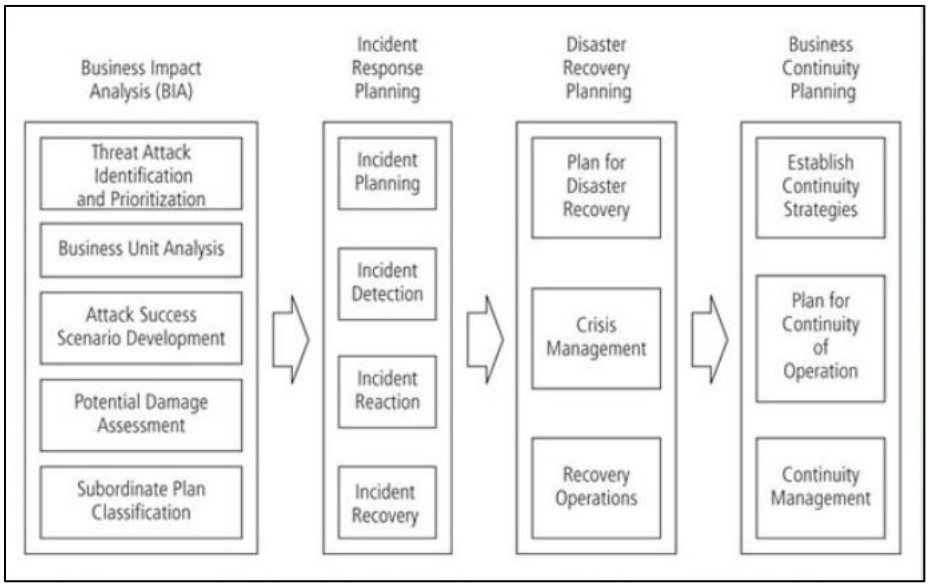

Figure 1: Tasks in Contingency Planning (Bradford, 2015)

The first phase is BIA, in BIA all possible attacks which can harm assets of the business are identified. Then according to the value and importance of assets, different assets are prioritized. Then a scenario is developed when distortion occurs.

Different distortions damage different assets of the business so, potential damage is assessed. Lastly, to protect the assets or mitigate the effect of the distortion subordinate plans are classified. Therefore, the process of BIA is completed.

Moving on, IRP is the next planning while developing a proper contingency plan. IRP focuses on takin immediate action when a distortion occurs. First, a plan should maid when any type of distortion occurs.

After plans are maid, the distortion should be observed and immediate action according to the plan should be taken. If this solves the distortion no further steps should be taken or else DRP should be started.

When the impact of an incident cannot be controlled by an organization, the incident is then called disaster. In disaster recovery planning, a plan is made where the ways to mitigate the impact made but it mainly focuses on saving human life.

After planning, crisis management is done which deals with the people involved during and after the disaster. Once crisis management is safely executed business continuity plan should be done and once the disaster is in control, recovery operations can be done at the primary site.

Business Continuity Planning helps business provide its service even if a disaster occurs. This is possible by re-establishing important business assets at alternate site. For choosing an alternate site different strategies can be used according to the need of the business.

After the strategy is maid, the service from alternate site is used to provide service to its customers. Now after using alternate sights the resources should be managed and similar services should be provided. Although, the service provided from the alternate site won’t be as good as the primary site.

Now once BCP and DRP is set, an organization will be able to react during and after a distortion according to the established plans. These plans will help an organization to fulfil its aim and objectives.

The objectives like safety of important assets, equal effort by all teams, implementation of plans, communication between primary and alternate sites,

and Data and Hardware backup will be fulfilled. Which leads to the aim of providing uninterrupted service is also fulfilled.

Moreover, prioritizing the assets of an organization which gives more value is important in an organization to provide uninterrupted service. If an organization's location is at a foody area, then the main service provider should be at the top floor. This is the way of prioritizing the need of the organization. Using antivirus and firewalls also protect the digital assets if used properly.

There are in total of 4 teams who involve in contingency planning (CP) and operations. Namely, Overall CP team, Incident Recovery (IR) team, Disaster Recovery (DR) team and Business Continuity (BC) team.

Every team has its own specific tasks when a distortion occurs. For illustration DR team is responsible for re-establishing the organization in the primary site. Also, BC team is responsible for providing service as soon as possible in an alternate site.

3. Literature Review

3.1 Case Study

3.1.1 Findings

Business Continuity Plan (BCP) of an IT company called Cantey Technology helps in providing uninterrupted services. The service included host services for more than 200 clients. A lightning struck the building of the IT company which destroyed the hardware and according to their BCP the client server was moved to a remote data centre which led to an uninterrupted service. (Rock, 2018)

Similarly, a German telecom company implemented a proper Disaster Recovery Plan (DRP). A dangerous fire was lit in the company facility which completely destroyed the entire switching center. Use of a system from Simba was used to control the fire. Around 1,600 employees of Simba came to control the fire. After six hours, the disaster was controlled, and the telecom service was back online. (Rock, 2018)

Also, In August 2017 a hurricane Harvey slammed into Southeast Texas. Over four days heavy rainfall led to 40 inches of rainwater. This resulted in flood which made physical access over the assets of Gaille impossible. The physical access was unavailable for three months. However, because of Business Continuity Plan of Galle, the data was stored in the cloud. This allowed the staffs of Gaille to remotely work, and the service was still available. (Rock, 2018)

On the other hand, In March 2018, a Ransomware attack was done in the city of Atlanta which displayed a bad planning. This attack was focused on the government computer systems of the city. As a response the computers were shut down for 5 days which led to the government departments to complete all paperwork by hand. The demand of the attackers was $52,000, when all was said done more than $17 million were spend because of this attack. This is an example of improper

establishment of BCP and DRP because there were more than 1500 vulnerabilities in the system of Atlanta government. (U.S. Attorney, 2018)

Similarly, in three hospitals in UK ransomware attack were done for five straight days. This led to cancelling more than 2800 appointments. Only serious patients were admitted. The main reason for the loss to the hospital was BCP was not set. The hospital officials misled the situation by saying it was a firewall misconfiguration which made the case more severe. So, BCP and DRP is very important in any organizations. (Rock, 2018)

Moreover, one of the most successful social media company, Facebook's service was for six hours. During a routine maintenance, the engineers had used a command which took down all connections in its network. Also, the Facebook's program audit tool had a bug and failed to stop the command that caused servers to go-down. There was not DRP or BCP for this case so, as a result the service of Facebook based applications were unavailable for six hours. Because of this outage a total of $66 million was lost. (BBC, 2021)

In order to avoid problems from disaster an electronic company in Georgia, the company implemented a FatPipe WARP at its main site and the old WARP was used in the secondary site. Both WARP in each site was connected by a fiber loop. A test of total site failover was done, and the company can use either WARP to operate. (Rock, 2018)

3.1.2 Analysis

Many Businesses and organizations over the years have taken the advantages of Business Continuity Plan and Disaster Recovery Plan. However, some of them fail to do so. When a firm has properly established BCP and DRP they are less likely to fall apart when a distortion occurs.

In the findings part to this case study, uninterrupted service was provided by an IT company called Cantey Technology. At the time of

disaster, the proper BCP helped the company provide uninterrupted service.

Similarly, in a German telecom company the DRP helped the company bounce back after the service was unavailable for six hours. An alert system of a fire-fighting team was called to stop the fire as soon as possible which was an act of DRP.

Also, in southeast Texas when a hurricane struck the city leaving 40 inches of water making physical access over the system impossible, the BCP of accessing cloud and remotely working was done in Gaille.

However, some organizations don't understand the proper need of BCP and DRP. And as a result, they face problems. For example, the government system of Atlanta city and hospitals of UK had vulnerabilities which was exploited by hackers which led to ransomware attack and lost millions of dollars.

More in this case, the lack of awareness of the system and the vulnerabilities of the system led to ransomware attack. If the government of Atlanta were aware about the vulnerabilities their system and took precautions by fixing those vulnerabilities, hackers would be unable to exploit the vulnerabilities and therefore the system would be safe.

Similarly, Instead of misleading the IT officials by the staffs at hospitals of the UK, if they provider accurate information the time consumed to fix the problem and loss would be less than the actual loss.

Similarly, in Facebook only a six-hour server down let to loss of millions of dollars. There was no BCP or DRP for this outage because nobody expected it to happen. So, plan should be made to cover every possible threat.

4. Conclusion

For conclusion, Business Continuity Plan (BCP) is the process of starting business operations in an alternate site. And Disaster Recovery Plan (DRP) focuses on resuming work in the primary site when a distortion occurs. The implementation of both BCP and DRP is equally important because different plans focus on different actions a business should take. Therefore, the concept of BCP and DRP helps as organization to provide uninterrupted service in any situation.

5. References

BBC, 2021. *Facebook down: Zuckerberg apologises for six-hour outage - BBC News.* [Online]
Available at: https://www.bbc.com/news/technology-58800726
[Accessed 2 January 2022].

Bradford, J., 2015. *Contingency Planning Things which you do not hope happen more frequently than things which you do hope. -- PLAUTUS. (C. 254–184 B.C.), MOSTELLARIA, ACT. - ppt download.* [Online]
Available at: https://slideplayer.com/slide/6270446/
[Accessed 30 December 2021].

Dey, D. M., 2011. *BUSINESS CONTINUITY PLANNING (BCP) METHODOLOGY –,* Dubai: IEEE GCC Conference and Exhibition.

MacNeil, C., 2021. *Business Impact Analysis (BIA): How to Prepare for Anything • Asana.* [Online]
Available at: https://asana.com/nl/resources/business-impact-analysis?utm_campaign=NB--APAC--EN--Catch-All--All-Device--DSA&utm_source=google&utm_medium=pd_cpc_nb&gclid=Cj0KCQiAq7COBhC2ARIsANsPATGotGMH_f8OLSsfhgmDeImX6ObqmW_cyxiy_WE8bP64WxAuqy30bSQaAqVAEALw_wcB&gclsrc=
[Accessed 30 December 2021].

Omar H. Alhazmi, Y. K. M., 2013. *Evaluating Disaster Recovery Plans Using the Cloud,* Colorado: IEEE.

Rock, T., 2018. *4 Real-Life Business Continuity Examples You'll Want to Read.* [Online]
Available at: https://invenioit.com/continuity/4-real-life-business-continuity-examples/
[Accessed 2 January 2022].

TechTargate, 2015. *What is contingency plan? - Definition from WhatIs.com.* [Online]
Available at: https://whatis.techtarget.com/definition/contingency-plan
[Accessed 30 December 2021].

U.S. Attorney, 2018. *Atlanta U.S. Attorney Charges Iranian nationals for City Of Atlanta ransomware attack | USAO-NDGA | Department of Justice.* [Online]
Available at: https://www.justice.gov/usao-ndga/pr/atlanta-us-attorney-charges-iranian-nationals-city-atlanta-ransomware-attack
[Accessed 2 December 2022].

6. Bibliography

Dey, D. M., 2011. *BUSINESS CONTINUITY PLANNING (BCP) METHODOLOGY –,* Dubai: IEEE GCC Conference and Exhibition.

Omar H. Alhazmi, Y. K. M., 2013. *Evaluating Disaster Recovery Plans Using the Cloud,* Colorado: IEEE.