IS5151 - Information Security Policy and Management

Semester 2 - 2018/2019

Business Continuity Plan and Disaster Recovery

Jagadeesh Chirumamilla	A0191509B
Maddi Kamal Divya	A0178511E
Rohaizad Bin Noordin	A0195026E
Xu Haodi	A0191531L
Li Jiachen	A0194979Y
Yare Feng Shui	A0194951U

Contents

1 Introduction

Over the years, technology has advanced rapidly, bringing convenience to different walks of life. Besides that, given the efficiency brought by technology, many companies started to computerized their work processes and functions. Accountants no longer use pens and papers to do their accounts, documents such as proposal, quotations etc. were typed using computer instead of handwritten on the paper and communications within the company and external parties were mostly done through email etc.

However, this also creates heavy dependency on technology. Although technology provides high reliability, things could also go wrong with different type of disruptions, generally categorized into man-made or natural disaster. Man-made disruptions could further divide into intentional or unintentional. Intentional man-made disruption could be Hacking, Terrorism, Act of Wars etc. Unintentional man-made disruption could be power outage, equipment failure, software errors etc. Natural Disasters, on the other hand, includes flooding, earthquakes, hurricanes etc.

As the above disruptions could happen at anytime and anywhere in the company, company must always ensure that it is ready to take on various kind of disruptions. In case of company failing to handle disruptions, the company could suffer from reputation damage, financial loss, discontinuation of the business or even fatalities.

A typical example of such cases is outbreak of computer virus, known as Northern Lincolnshire and Goole Trust, in United Kingdom's Hospitals happened on November 2016. According to the investigation, the hospitals did not have any business continuity plan in dealing computer virus outbreak and this outbreak of computer virus had crippled the hospital's network. As a result, the hospitals were not able to perform daily task for a few days and incoming patients were turned away and send to other hospital for treatment.

In this white paper, various BCP and DRP available tools and the usage of the tools will be explored. Besides that, the challenges faced in while selecting the tools in BCP and DRP will be discussed. Lastly, the future trend of the BCP and DRP tools will be discussed to wrap up the entire white paper. The following paragraphs will define the business continuity and disaster recovery definition in this report.

Business continuity is the ability to maintain operations and services in the event of disruptions. It requires the availability of computing, application and network services, physical network accesses and user and client accesses to that infrastructure. Continuity of an application is achieved by failing over those services locally within the same datacenter or to a remote datacenter and is measured in seconds or less.

Disaster recovery is the activity of recovering IT systems after a natural disaster or man-made interruptions. It requires manual procedures to bring the technology environment to an operational state. Infrastructure used for disaster recovery include virtualization, server hardware, network services, remote facilities and backup related processes.

2 Motivation and Importance

According to the research results of Gartner Group, close to one third of the company's operation could be ceased within three months if the company's data centers and information infrastructure is malfunctions for more than 10 days and up to 90% of company could be shut down within a year. Several researches have supported the idea that a more comprehensive approach to pre-disaster planning would be more cost-effective in the long run. For every one dollar spent on disaster mitigation like DRP, society saves four dollars in disaster response and recovery costs. According to 2015 disaster recovery statistics, one-hour downtime costs small companies $8,000, medium-sized organizations $74,000, and large businesses $700,000. As a result, in order to ensure minimal losses, companies should attach great importance to BCP and DRP.

With these significant impacts, one may wonder what are the BCP and DRP tools available in the market that could provide security to the company? Given the different type of tools available in the market, how can the tools be used in the company to mitigate disruption risk within the business lifecycle?

With the above motivation, this white paper will list down the different type of tools employed in BCP /DRP will be covered, the usage of tools and various worth noting best practices will be explained. However, considering the variation that may be used in different industries and departments, this report will focus only on the general and essential tools applicable to all the industry i.e. data protection.

3 Current state of the art

3.1 Current Technology

The key elements of a business continuity plan are essentially resilience, fast recovery and contingency plan to the company system to ensure business can remain operable. Resilience enables us to quickly adapt to disruptions while maintaining business operations and safeguarding overall brand equity, people and assets and this can be achieved by designing critical function and infrastructure with various potential disasters in mind. This include staff rotations, data redundancy and maintaining. Fast recovery aims to restore business operations rapidly after an interruption or disaster. This is done by setting various recovery time objectives for the various systems and networks to prioritize what need to be recovered first. As for contingency plan, the course of action facilitate company to respond effectively to impactful future events and it contained various procedures for the various scenarios that could happen.

There are various technologies that are used by BC and DR professionals and in this paper, we will be discussing on four different technologies that are used by professionals that support the business continuity planning.

3.1.1 Server virtualisation

Virtualisation reduces the number of physical servers needed while increasing the utilisation level of the other servers. Server virtualisation partition a physical server into multiple servers isolated virtual environment. Each with capabilities of operating and running on its own machine.

Server virtualisation bring about various benefits.

a) **Lower number of physical servers:** Lower server reduces the hardware maintenance costs

b) **Increase space utilisation efficiency in data centers:** Consolidating server will save space in the data environment

c) **Less dependency between applications:** Virtual servers prevent one application from affecting another application when there are changes and upgrades made to the servers.

d) **Multiple OS:** Various operating systems can be deployed on a single hardware platform through server virtualisation.

3.1.2 Cloud disaster recovery

Cloud computing virtualized resources as a service over the internet. This service provide business applications online accessed via web browsers. Various key features of using cloud includes: the ability to recover data in the cloud, unlimited scalability, pay-per-use billing model and secure and reliable infrastructure. This cloud disaster recovery have various ways of implementation such as in-house, partially in-house or purchased as a service.

3.1.3 Green technologies/Going Green

Data centers require a large quantity of power and electricity to allow the physical servers to remain cool. However, some companies have placed their data center in countries with a chillier environment and climate that would help reduce the overall power input costs by reducing the need of cooling equipment. Other ways of consolidating the servers includes reducing floor space generating renewable and using recycled energy.

Various examples of green technologies:

1. Free air cooling
2. On- site wind generation or use of renewable energy
3. Low-power servers
4. Data centre virtualisation and consolidation
5. Cloud computing
6. Modular data centres.

3.1.4 Data deduplication

Data deduplication lowers the volume of data backup by a significant amount. This process helps reduce redundant data by identifying duplicate blocks of data in the disk. A reduced amount of back up data result in smaller amount of information needed to be sent over wire, thus, less information is transferred during disaster recovery. With less information in the system, application would be smaller and are operated on fewer servers, then, it will be easier for the team to do disaster recovery procedures. Deduplication copy only unique new data to the backup disk. Benefit of deduplicating includes reduced disk storage requirements, reduced bandwidth requirements for site-to-site backup and faster recovery operations.

3.2 Current Infrastructures

Uninterruptible Power Supply, known as UPS, is a common tool integrated in the company infrastructure. UPS is essentially an external battery that is part of the circuit of company key infrastructure and the power source. UPS is usually used to protect computers, Data Centre, telecommunications equipment and other critical equipment that may cause injuries, fatalities etc. Since the key infrastructure is run by electricity, a single point of failure could arise in an event of electricity outage, unstable voltage etc. As such, UPS is used to replace main electrical source to ensure business continuity and reduce financial loss in an event of power outage. Till date, UPS remained to be one of the effective measure to combat with power outage, unstable voltage in the key infrastructure.

Hot site, warm site and cold site are an alternate site used by company in ensuring business continuity in case of inoperable. The difference between the sites is the availability of infrastructures and facilities (such as equipment, computer, server and etc.). In cold site, there is no infrastructure and facilities. As the temperature goes up, the readier the infrastructure and facilities are. With the availability of the alternate site, this allows company to recover and continue their business from the disaster in the shortest possible time. Despite that, the cost of the site goes up in accordance with the availability of infrastructure and equipment in the site. The selection of the site is dependent on company budget and careful planning is required to ensure company remain operational in case of disaster. However, with the improvement in laptop technology seen in the recent years, company have found workaround for the need of using hot site. Company is using laptop for work increasingly and invest in Virtual Private Network (VPN). As a result, this reduces the need of needing a hot site.

4 Current challenges and issues

4.1 Establish the business continuity plan

The business disaster recovery goal is not clear, the information system disaster preparedness coverage is insufficient, additionally the disaster preparedness resources effective guarantee is insufficient. The lack of risk assessment and business impact analysis, as well as the lack of cost and benefit measurement of business interruption loss and disaster preparedness construction investment, has led to the blind investment, lack of planning and insufficient coverage of disaster preparedness systems in the construction of disaster preparedness systems and scientific and technological emergency response systems. Although most companies have established disaster preparation centers, the business classification and differentiated business recovery goals are not very clear. Some disaster preparation centers only focus on the level of core data like accounts and production protection. Once a disaster occurs, it is difficult to achieve the recovery of important real-time data for business processing, and important customer data.

4.2 Maintain the business continuity plan

Despite the pressure of national or regulatory policies, operation needs, and clients' demands, companies nowadays lack subjective will, hold insufficient understanding of the importance and the value of business continuity management and don't form an effective BCM system. They may think that "large investment, small return". Since the business continuity plan is not regarded as the core business in most companies, there may be some gaps or hindrance in management part as follows at most times.

a) **Lack of clear decision hierarchy.** The situation that people don't know who is in charge or who has the power to make decision may exist when there is an emergency.

b) **Not implement test plans.** Test plans mean a regular comprehensive emergency simulation, including security exercise, urgent communication and workspace recovery processing. And the next significant step is also usually neglected, which is auditing the test results and striving for continuous improvement against application available target and personnel security.

c) **Not enough training.** Companies pay more attention to enterprise business and focus less on staff training based on security process, which results in knowledge deficiency about emergency response and resource access.

d) **Lack of updated plan.** Most companies are likely to ignore the variation of application, business institution, business priority, operation and other small but important elements under the complex cause of business interruption.

4.3 Maintain the disaster recovery plan

Maintaining the DR Plan is an overwhelming challenge for most companies, since it needs continuous support and update. The biggest challenge is that the DR Plan not only executed during the deployment process, but also required continuous maintain and update after completing the deployment process. Commonly, the DR plan contains a plan for each application associated with data, user connectivity and the sequential steps for recovery in the event of a real disaster. With applications changing and upgrading, the task of updating the DR Plan in order to keep it effective is important for reflecting the change of infrastructure features and business processes of IT systems.

4.4 Technical implementation bottlenecks

There may be technical and development issues and the following is a failure case of The California Department of Motor Vehicles (DVM) in business continuity plan and it demonstrates how the problems happened. Due to the computer outage, several DVM California offices closed and drivers had nowhere to get their licenses. It seemed that the single power shared by the primary backups systems and the secondary backups systems shut down, which led to disaster of DVM operations. In the field of backup and disaster recovery, different situations in regard to clients' expectations, demands and some objective factors may require different solutions so it may be hard to consider completely. Once companies took use of inaccurate technology, this would not only have backup role, but in the event of failure could have greater losses. It would be a challenge but also an opportunity that more mature technologies such as cloud need to be applied to the actual process more appropriately.

4.5 Meeting RPO/RTO

Recovery point objective (RPO) is the amount of data or transactions that is acceptable to be lost when restoring from the last backup, and Recovery time objective (RTO) is the amount of time to restore the application to a working state. For traditional backup software, their RPO/RTO might be 24 hours due to the compute resource limitations for backing up processes. While this speed might be adequate for some backup scenarios, DR generally has more demanding in RPO/RTO. However, meeting a high-efficiency RPO and RTO require a lots of compute resources and steady hardware support.

4.6 Regulatory Issues and High Costs

It is well acknowledged that most customer-facing and real-time applications usually demand a shorter PRO and a faster RTO, since the loss of data and downtime can have a severe impact on the business and result in a high risk of the company. For many traditional DR solution, it could contain some alternative methods with fewer resources and smaller workload. For instance, several technologies according to Array-based LUN or volume mirroring could backup every 30 minutes. However, those kinds of techniques required sufficient backup capability to satisfy regulatory and operational requirement for data protection, such as backup storage, backup catalogue, individual VM or file recovery. In addition, many DR solutions required specific secondary data center and servers to handle the duplicated data in the event of the disaster. Therefore, all these semi-custom DR plan and bandwidth for data movement will lead to a high cost, which could out of the financial reach for many companies.

5 Future Trend

5.1 Migrating to the cloud - Providing services and infrastructure.

The cloud is a viable disaster recovery service tool that is emerging. Since cloud computing relies on hardware-independent virtualization technology, it is possible to quickly backup data, applications, operating systems to a remote cloud or a remote data center. Increasing the speed of uploads and downloads of critical components lead to faster recovery times for businesses. Now a days many of the organizations are moving towards cloud. One of the advantages of cloud is the cloud disaster recovery which helps in storing the multiple copies and replication of records that helps in backup of records and restoring when needed. Cloud BC/DR helps the organizations to recover data and implement the failover in event of any disaster. Cloud environment for Business continuity and disaster recovery can be implemented in three strategies On-premise cloud as BC/DR plan, Primary BC/DR cloud provider and alternative cloud provider. (LADEJI, 2019)

5.1.1 A Unified Version of Data Backup and Disaster Recovery - On-Premise Cloud as BC/DR Plan:

Backup and Disaster Recovery work hand in hand in this model from the Organization's perspective. In this the enterprise infrastructure which supports the business of an organization will in the on-premise. The organization have to find an alternative cloud provider who will deliver services on the event of disaster by continuously backing up the Organization's data. Recovery point objectives have come down to seconds with advanced data protection techniques by provisioning Point-In-Time Recovery (PITR) capabilities. These recovery strategies provide Organizations to effectively restore data from a point in time merely seconds before disaster strikes which is way superior than the earlier approach which revolved around a single data backup. Additionally, it delivers convenience, flexibility and economic value as IT investments can be diverted toward single and scalable hybrid platforms. Here organizations have to carefully review the service level agreement to ensure what all services will be available and business requirements are met.

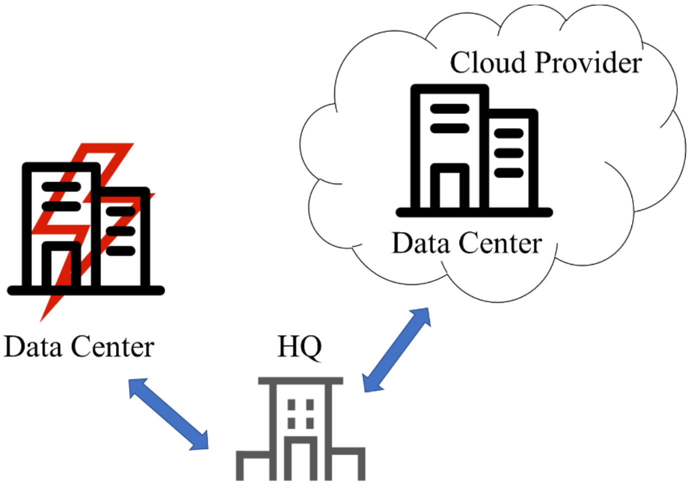

Figure 1: On-premise cloud as BC/DR plan

5.1.2 Cloud Infrastructure is the New Trend - Cloud user, Primary BC/DR cloud provider:

In this strategy, the organization's enterprise infrastructure is already moved to the cloud. The current cloud provider act as primary agent for BC/DR implementation. This model has all the capabilities mentioned in the above model and in addition, it remarkably reduces the data center’s capacity requirement, platform management. Providers are already focusing to allow de-duplication of data backed up in virtual environment to offer transformed levels of scalability. Vendors are providing solutions that does automated integration of newly created VMs and migrated VMs with the backup software. This model may pose many security threats as the data is not in house, but it is less considerate when compared to the advantages provided by this model.

In this scenario, the regional failures can be handled, and it depends completely on the providers capabilities. As the focus in more on the resources and capability of the cloud providers, organizations have to carefully select the cloud provider.

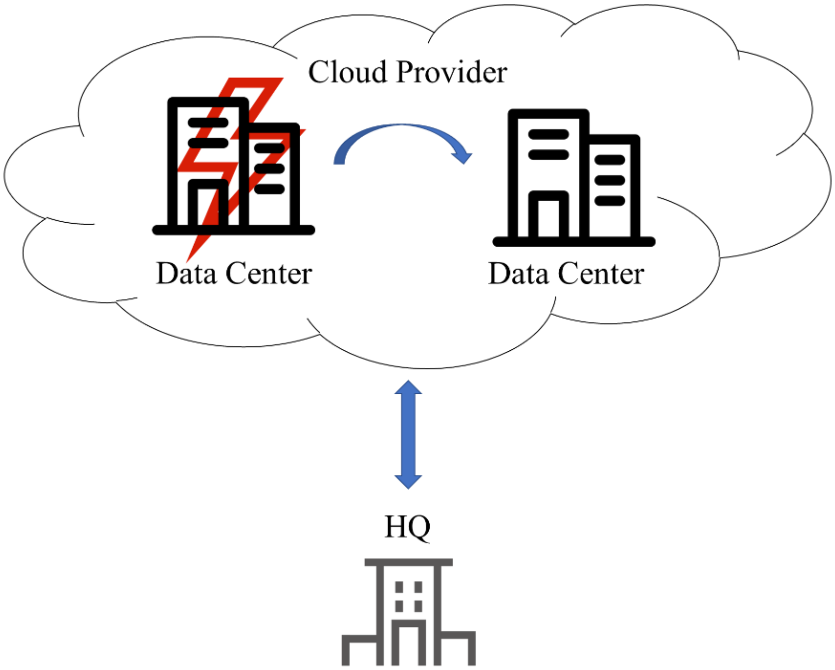

Figure 2: Primary BC/DR cloud provider

5.1.3 Hybrid Cloud - Cloud user, Alternative BC/DR cloud provider:

Relying on a single vendor is now a thing of the past. Organizations are increasingly opting for vendor-agnostic models to avoid lock in. Hybrid cloud is at the future of this evolution.

In this strategy, the organization’s infrastructure is already with one cloud vendor, but the business continuity and disaster recovery will be provided by the alternative cloud provider. In this scenario, the complete failure of the primary cloud can be handled. This approach may occasionally increase the complexity of data protection as the services will be handled by the alternative cloud provider. Organization need to check the failover time as resource switching from one cloud to another cloud will take time and functionalities of the current cloud and alternative cloud may differ, but this certainly makes business continuity more effective. In this case immediate involvement of the business users are required to assess the business impact.

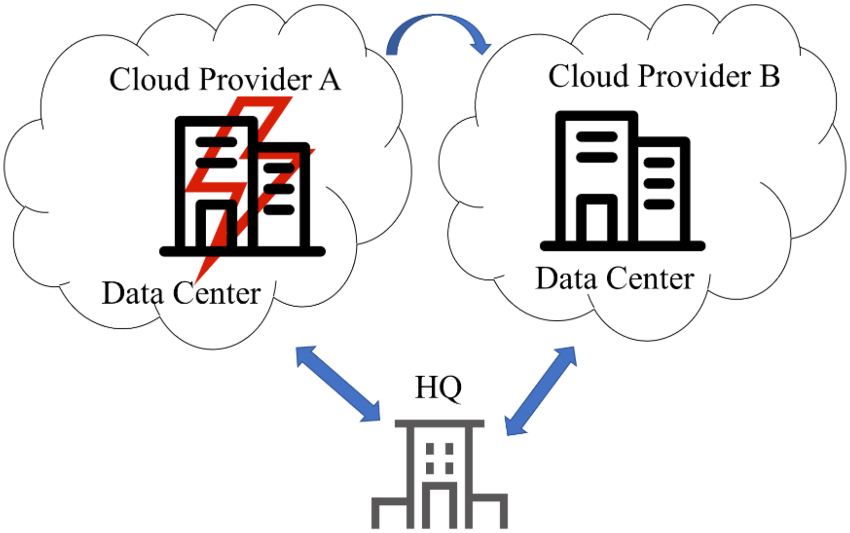

Figure 3: Alternative BC/DR cloud provider

This helps the smaller organizations to implement the robust disaster recover while reducing the assets expenses as they no need to invest on the new infrastructure, network and data center space. As the cloud sells the services as pay-for-use model, cost depends only on how much storage and bandwidth an organization going to use.

Before implementing the Cloud BC/DR organization has to check (Rouse, 2019):

a) Whether the organization has enough bandwidth to access the cloud as data movement from cloud depends completely on network

b) Does organization have no problem to save their data on third party cloud and what encryptions they are going to use to save data on cloud.

c) Evaluation of the important assets which need to be protected and restored.

Cloud BC/DR automatically handles the failover by switching to alternative site. Once the original site is working fine it will shift the workload in failback process.

However, organizations have to tests these failover and failback as a drill at regular interval of times for example if the application is mission critical then the drill should happen every quarter. If it is not mission critical, they can have drill on alternative quarters.

5.2 Virtualisation

Normally, one of the BC/DR solutions involves creating the same infrastructure at remote site as that of the primary site. Data will be synchronized by replication. This kind of setup will be expensive and time consuming. To solve some of this issue we can go for virtualization.

With the help of virtualization, a software will simulate the existing hardware to create a virtual computer. A single server can run more than one virtual system, different operating systems and applications.

If an organization is implementing the virtualization then they need to assess first how many servers, they need to backup and create full image of information this is what we call as server consolidation ratio. The first important is given to the servers which are hosting mission critical information. For example, we can consider email service, the servers which are hosting email services are critical to an organization and some of the inhouse built applications. These types of applications should be restored and recovered quickly.

With virtualization environment, failover takes very less time as the images exists in real time, once the primary setup is working failback can be easy but one of the drawbacks of this is the data integrity as the databases of each setup is different, additional efforts from the employees is required to move data from DR system to primary setup (Kirvan, 2019).

Another way of implementation is using the docker containers which helps to reduce the setup time and uses the light weight containers. The working containers can be backed up regularly and it is easy to create images from the containers and can be pushed to the repositories. These images can be pulled from repository anytime and by using just few commands containers can start running.

Some benefits of using the virtualization (Business Continuity: Virtualization, 2019):

a) **Server Utilization:** As single server can host multiple virtual images; the server resources can be shared effectively between all images by this complete server utilization is achieved.

b) **Backup and recovery:** It is easy to take backup of virtual machines compared to machine by machine and recovery time will be less in compared to individual machines.

c) **Energy conservation:** Fewer servers will reduce the operational costs.

5.3 Disaster Recovery as a Service (DRaaS):

Disaster recovery services (DR) prevent costly service disruptions from causing manmade or natural disasters. The notice of failure may be manual or automated. The operation of DRaaS can continue until IT can repair the on - site environment and issue a failback order.

Organizations can specify a recovery point objective, a recovery time target and a recovery data region during the DR test. Disaster Recovery as a Service provides the organization with the capabilities to generate a scenario for disaster recovery test. In the event of a failure, organizations can test business continuity by planning strategies to balance disaster recovery objectives, such as high data reliability, low backup costs and short recovery times. Even without a real disaster, DRaaS allows organizational applications to run on virtual machines (VM) during production time. DRaaS is useful for small and medium and - sized organizations that lack the necessary expertise to provide configure and test an effective disaster recovery plan.

5.3.1 Challenges faced in Disaster Recovery as a Service (DRaaS)

a) **Handling Failures:** A service provider usually manages all its DR customers on its server pool by multiplexing them, assuming that not all its customers experience simultaneous failures. Service Providers must therefore ensure that the provider has a number of free servers to meet peak needs of all its customers.

b) **Migration and Cloning back:** After a successful DR test, care needs to be taken to restore the application to its original site after a disaster . In order to support this, service providers must identify additional functionalities and optimize migration techniques.

c) **Revenue:** A DRaaS value is not known until a Disaster actually happens. But Organizations have to continue to invest in DRaaS and there is still uncertainty in recovering all the lost data in case of a failure event.

5.3.2 DRaaS advantages

a) **Multisite:** Duplicate resources to several different sites to ensure a continuous backup in the event of a failure at one or more sites.

b) **Array agnostic:** DRaaS replicates has capabilities to provide service to any vendor or platform.

c) **Granular or comprehensive:** Organizations can make feasible requirements by choosing what data needs backup and can reduce costs or expenses under flexibility protection.

d) **Additional Services:** With the competition in the market, few providers are coming up with providing containers for each organization to achieve isolation and security. Many products are sending tapes and disks to their customers as an additional service to handle the bandwidth issues for the first-time full backup.

5.4 Outsourcing

As the Business Continuity is costly and time consuming, Outsourcing will avoid unknowingly putting an organization at risk. Keeping an eye on the new evolving trends is confusing without proper level of expertise. It is nearly impossible to manage business continuity effectively, especially for small to medium business organizations. To fill the critical gaps and implement stronger and more dependable BC/DR technologies, outsourcing will be best. Reducing the cost of maintenance will provide the organization with the opportunities to focus on other tasks such as enhancing the defensive mechanisms. Outsourcing provides advantage as below.

a) **Transferring the Risk:** To transfer the risk, companies are handing over control of non-critical and critical business processes to third party providers and outsourced solutions.

b) **Infrastructure as a Service (IaaS):** Business organizations depend heavily on third parties to provide services such as web hosting, production testing environment and development platforms. Most service providers try their best to improve the quality of services and use different data storage techniques and avoid duplication.

c) **Outsourcing provides compliance guidance:** As there are different regulations to be followed, outsourcing will assist the organization in understanding these laws, how to maintain compliance and what actions to take if penalties are enforced.

d) **Risk Assessment and Mitigation:** Outsourcing helps to implement risk management policies into an Organization's business continuity plan. They also help to implement the defense and mitigation techniques.

By outsourcing, companies can noticeably reduce their internal disaster recovery needs. But organization's must be careful in differentiating critical and non-critical business processes before outsourcing to third party providers to ensure security and isolation.

5.5 Underwater Data Centers - Microsoft 's Project Natick

To meet the demands of power and cooling, Microsoft has set up a data center with the size of a shipping container as initial project in Scotland's Orkney Islands. The motive is to make the data center cheaper in the long run and make it more sustainable. The towns and cities that are closer to data centers in the underwater provides high speed access. Microsoft is leveraging the technology used to cool submarines. This resolve the power problem that requires to keep the servers cool for long time. The water flow rate should discourage the growth of the barnacle. This cooling system could deal with very high-power densities, such as those required for high - performance computing and AI workloads using GPU - packed servers. The tidal energy in Oceans act as reliable battery storage to get a smooth roll across the full 24-hour cycle and the whole lunar cycle, thus contributing to business continuity even if there is a power disruption.

This data center has 12 racks and 864 servers and FPGA boards and fits into the size of the container. Natick datacenter functions like thousands of high-end consumer PCs and has adequate storage space which can hold five million movies.

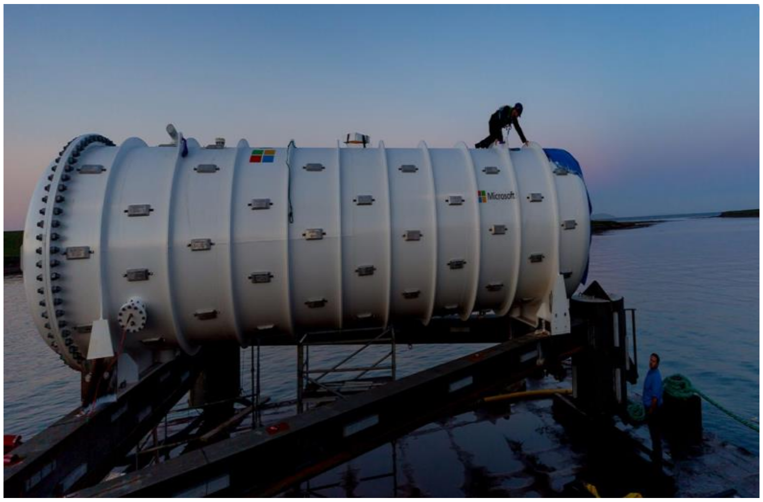

Figure 4: Microsoft’s Project Natick

5.6 Movable Data Centers

Many companies are investing in mobile data centers. The mobile data center is assembled in well - built containers of the size of regular modular containers. The average size varies between 20 ft, 40 ft and 60 ft. For the conventional stationary data center, containerized mobile data center is an alternative. These Data Centers are loaded with computer equipment and can be transported using standard shipping methods as it is built in a container. These data centers are weather resistant and insulated and so, can be deployed in environments like tundra or the desert.

These containerized data centers can provide high value when the data center is required to be moved to move from one place to another during a disaster if the disaster is predicted earlier. Another use case is to supply the data center resources to continue the business in the case of high demand. For example: Hosting an Olympic event demands high computing resources and the country or region may not need it after the event is completed. Mobile data centers come to rescue in these cases. Another use case for these mobile data centers is in Defense Forces where the data center needs to be mobile and reliable in the time of need. (In case of wars or any attacks military can use these movable data centers to hide their data and perform secret operations).

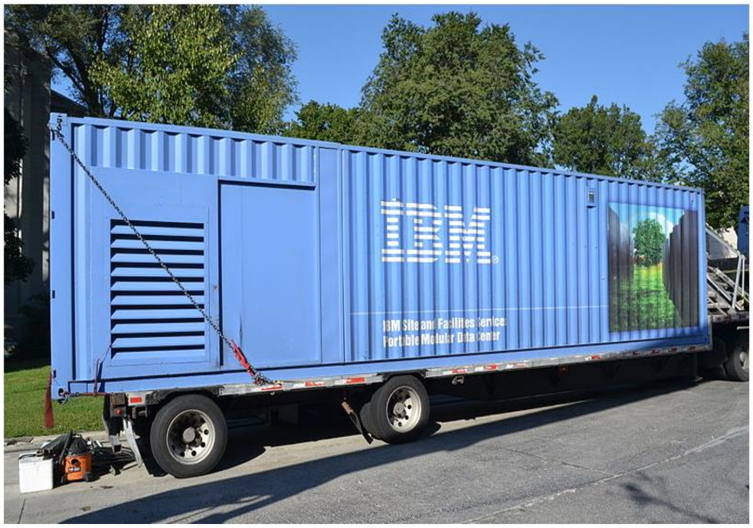

Figure 5: IBM’s movable datacenter

The above future trends are implemented by Pioneers and we hope that these can be affordable for small and medium scale businesses to continue with their businesses.

References

1. AIG. “Building a Business Continuity Plan. Guidelines for preparation of your plan”, [Online], May, 2013, accessed at https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/property-insights/business-continuity-planning-guidelines-for-preparation-of-your-plan.pdf in February 2019.

2. Timothy W., Emmanuel C., K. K. Ramakrishnan, Prashant S., Jacobus V.“Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges” in Proceedings of the Conference on Hot Topics in Cloud Computing (HotCloud), 2010.

3. Witter Publishing Corp, CPM/KPMG Business Continuity Benchmark Survey, 2002.

4. Tracy Rock “6 Real-Life Business Continuity Examples You ‘ll want to read”, [Online], December 20, 2016, accessed at http://invenioit.com/continuity/4-real-life-business-continuity-examples/ in February 2019.

5. Krebson “Computer Virus Cripples UK Hospital System”, [Online], November 2, 2016, https://krebsonsecurity.com/2016/11/computer-virus-cripples-uk-hospital-system/ in Mar 2019.

6. Paul Kirvan “Five key business continuity technology to support BC planning in 2010”, [Online], 2010, accessed at https://searchdisasterrecovery.techtarget.com/feature/Five-key-business-continuity-technologies-to-support-BC-planning-in-2010 in February 2019.

7. LADEJI, O. “BC/DR Strategies within a Cloud Environment”, [Online], February 1, 2017, accessed at https://www.drj.com/articles/online-exclusive/bc-dr-strategies-within-a-cloud-environment.html in February 2019.

8. Joe Anslinger “*Business Continuity: Virtualization*”, [Online], April 5, 2016, accessed at https://www.ltnow.com/business-continuity-virtualization/ in February 2019.

9. Rouse, M. “cloud disaster recovery, *Cloud-based backup: Best strategies and practices*” , [Online], July, 2016, accessed at https://searchdisasterrecovery.techtarget.com/definition/cloud-disaster-recovery-cloud-DR in March 2019.

10. Kirvan, P. F. “How server virtualization benefits disaster recovery”, [Online], March 2009, https://searchdisasterrecovery.techtarget.com/feature/How-server-virtualization-benefits-disaster-recovery in March 2019.

11. Oregon Natural Hazards Workgroup “Post-Disaster Recovery Planning Forum: How-To Guide, Prepared by Partnership for Disaster Resilience”. University of Oregon's Community Service Center, 2007.

12. Pronto Marketing “The Importance of Disaster Recovery”. [Online], January 27, 2016, accessed at http://www.techadvisory.org/2016/01/the-importance-of-disaster-recovery/ in March 2019.

13. Saleh H. “Uninterruptible Power Supplies - the Cost and Risks of Not Having Them”, [Online], March 27, 2018, https://www.bapcs.co.uk/uninterruptible-power-supplies-the-cost-and-risks-of-not-having-them/ in February 2019.

14. Rouse M., Bergener K., “hot site and cold site”, [Online], November 2010, accessed at https://searchcio.techtarget.com/definition/hot-site-and-cold-site in February 2019.

15. Anexinet “4 Major Challenges with Traditional Disaster Recovery”, [online], Sep 14, 2017, accessed at https://www.anexinet.com/blog/4-major-challenges-traditional-disaster-recovery/ in February 2019.

16. Livia Alexandra Stancu. “DMV California Learns Disaster Recovery Lesson, Nov 2016”, Recovery Zone [Online], Nov 02, 2016, accessed at https://blog.storagecraft.com/dmv-california-disaster-recovery-lesson/ in February 2019.

17. Yongxiang S., Jing X., “On business continuity audit”, China Audit, July 2010, pp. 49-50

18. Rock T. “2018 Business Continuity Trends to Watch”, [Online], April 17, 2018, accessed at http://invenioit.com/continuity/2018-business-continuity-trends-2/ in February 2019.

19. George Crump. “Developing a complete RTO/RPO Strategy for Your Virtualized Environment”, Storage Switzerland, LLC [online], November, 2014, accessed at https://www.starwindsoftware.com/whitepapers/developing-a-complete-rto-rpo-strategy.pdf in February 2019.

20. Adeline Wong “Some Future Trends in Backup and Disaster Recovery” ,[Online], November 8, 2017, accessed at https://www.cloudbacko.com/blog/some-future-trends-in-backup-and-disaster-recovery/ in March 2019.