International Journal of Advanced Engineering, Management and Science (IJAEMS)
Peer-Reviewed Journal
ISSN: 2454-1311 | Vol-11, Issue-4; Jul-Aug, 2025
Journal Home Page: https://ijaems.com/
DOI: https://dx.doi.org/10.22161/ijaems.114.35

Business Continuity & Disaster Recovery

Suhail Kausar

suhailkausar@live.com

Received: 20 Jul 2025; Received in revised form: 19 Aug 2025; Accepted: 23 Aug 2025; Available online: 28 Aug 2025

Abstract— *The world around us is moving at an extremely fast pace than ever before and Information technology plays a pivotal role in driving this momentum forward. With its growth and innovations, the biggest challenge information technology brings is its Security, which is commonly known as Cyber Security. From Small Organizations to massive government infrastructures, Everyone takes exceptional measures to prevent cybercrimes So that businesses can continue to Operate Smoothly. This paper mainly focuses on Business Continuity & Disaster Recovery after a Cyber Attack. It also explains the latest Cyber Security Techniques, trend changes & Threats.*

Keywords*— *Cybersecurity, Information Technology, Business Continuity, Disaster Recovery, Threats

I. INTRODUCTION

As of 2024, 5.4 billion people globally have access to the Internet. There is an Estimated 2.5 quintillion (2.5 million Tera Bytes) of data created every day. With each click, Swipe, or share, businesses are using that data to make decisions in the future. Businesses have real-time data from any virtual source and then combine that to make smart decisions. Managing that much amount of data is a big ask but securing it is an even bigger challenge. From booking a Taxi to transferring money, Today every part of our lives is dependent on information technology, it's estimated that 70% of commercial transactions are done online today and with these emerging technologies we are unable to protect our information in effectively ways and cyber criminals take full advantage of that.

The answer to this problem is cybersecurity. Protecting Critical information & infrastructure can be achieved by Enhancing Cyber Security which is crucial to every nation's Security & economic well-being. Cyber experts spend the majority of their time & resources on tightening the security. Cybercriminals are not sitting idle waiting for you to make a mistake; they are proactive and highly motivated. In the cyber world, the criminals are always one step ahead. As businesses can't afford a second of downtime, In this paper, we will talk about Business continuity & disaster recovery which is an organization's ability to maintain or quickly resume acceptable levels of product or service delivery following a cyber-attack that disrupts business operations.

II. LITERATURE REVIEW

With the sophistication and frequency of cyber attacks growing rapidly, in modern times cybersecurity has gained a center stage for the businesses. Business continuity planning has become core part of modern day organizations and disaster recovery to achieve resilience from cyber security incidents. According to Business Continuity & Disaster Recovery by Susan Snedaker BCP focuses on the sustainability of core business operations during the incidents & crisis while DR is mainly responsible for recovering data and IT infrastructure after a cyber security incident or natural disaster. These approaches setup the basis of minimizing to no operational disruptions and securing revenue in the event of cyber events.

Importance of BCP and DR within Cybersecurity

The frequent worldwide cyber-attacks, as well as unusual Small, Medium & large cyber disasters in Organizations, have shifted the focus away from the traditional disaster recovery which is by no means enough to control unforeseen circumstances. There must be educated plans ready for business continuity. In Tech terms we call it BCP or business community plan. Disasters can occur for multiple reasons such as Natural Disasters, Technical Failures, cyber-attacks, Human Error, etc. The seemingly unpredictable uniqueness of the disasters demands dynamic, real-time, efficient, and cost-effective solutions, hence making BC extremely suitable. It is therefore extremely important to ensure that the correct procedures, policies, and plans are in place to protect an organization’s ICT infrastructure and data. Business continuity aims to keep the organizations running, regardless of the potential risk, threat, or cause of a disaster.

Susan Snedaker explains that BCP and DR strategies remain one of the most important factors in the current digital world, hence enabling all forms of businesses to quickly move out of cyber incidents and reduce both operational and financial losses. Because we understand that businesses have become so interconnected that no form of downtime will ever be affordable.

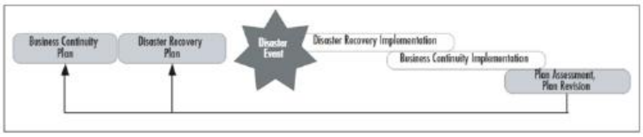
Best Practices and Frameworks for BCP and DR

The literature highlights a few best practices for implementing very effective BCP and DR frameworks. The most important part of any BC is the formational structure of recovery metrics, commonly known as Recovery Point Object (RPO) & Recovery Time Object (RTO). Recovery time objective (RTO) is the amount of time it takes to recover from an outage (scheduled, unscheduled, or cyber-disaster) and resume minimal or normal business Operations. Recovery Point Object (RPO) is the time in the past when your data can be restored from the backup. Let's say a 5-minute RPO means that in case of a disaster, you can recover your data from the recovery site that was backed up 5 minutes earlier.

Business continuity often requires Zero downtime which essentially is extremely costly but more often than not the cost of a disaster outweighs the cost of Zero downtime. The key element for business continuity planning is how much of a disruption a business is tolerable and what are they willing to spend to avoid disruption. If huge costs weren't a factor every business in the world would want fully redundant & zero downtime in their ICT environment. But Money is the main player here. A small business with a revenue of 2 Million USD per year will be spending approx. a hundred thousand dollars per year for a fully redundant system might not be justified but if a 5 billion-dollar revenue business is spending a million-dollar investment in fully redundant systems it might well be justified because a small disruption/attack might cause their business loss of millions of dollars, so there is nothing like “one size fits all” approach. We can conclude that the BC/DR plans must be appropriate to your organization’s size, budgeting & financial impact in case of a disaster.

The next step in planning is to look at the business processes used by the companies is in day-to-day operations. These processes need to be evaluated and prioritized in business-critical order. What processes are critical to the ability of the company to conduct operations? What is the minimum & maximum impact of a certain disaster on a business process? What processes can be put on hold during an emergency? Timing is another critical factor, for example, if a bank's ATM services are disrupted during the start of the month on Salary Day, the impact could be far more than the same service disruption happening in the middle of the month.

Susan Snedaker says that one of the most Critical part of BC/DR planning is to look at your use of technology and as per of implementation team, you need to understand which elements of your environment are vulnerable to which types of disasters. For example, An electricity outage will impact all the technology in a data center but considering there is a battery backup for servers & network equipment, no power for air conditioning in a country like the United Arab Emirates will quickly overheat all the equipment.


Business Continuity Plan
Disaster Recovery Plan
Disaster Event
Disaster Recovery Implementation
Business Continuity Implementation
Plan Assessment, Plan Revision

A bad plan or incomplete plan is often worse than no plan at all. Now I will go through a case study of a disaster where I was first hand witness of events.

III. CASE STUDY

Arab Authority for Agricultural Development and Investment Data Center Disaster

Organization Introduction

Arab Authority for Agricultural Development and Investment known as AAAID was Established in 1976, with head Quarter in Khartoum, Sudan. The AAAID is composed of 21 Arab member states which contribute to its capital. It Contributes to the Capital of 52 Major Agricultural Companies Across 12 Arab Countries. AAAID Data center was hosted in their Head office building in Capital City of Sudan, Khartoum.

Background

From 1989 to 2019, Sudan was ruled by military and was somewhat a stable country. But after 2019 mass protest, a reform path was laid out for civilian government to rule the country. With different Stake holders making their best efforts to come into the power the country, the situation was moving towards destabilization. At this point in time AAAID doesn't have any DR or business continuity solution in place.

Post 2019 Protests: In a Board Members (Consist of different Arab states sectaries of finance & agriculture ministries) meeting later in 2019, with keeping in mind on the current mass protest situation in Sudan, an agenda was proposed to setup a DR in another Country outside Sudan. The proposed location was in Dubai, UAE where AAAID already has a regional office. However when the financial cost of DR was brought to table, most members voted against the DR setup.

2021 military coup: As the fight to power continued which kept leading the country towards further destabilization. In Oct 2021, Military once again took over the country. Following the coup, mass protests erupted across Sudan. At this point AAAID realized the situation in Sudan is getting out of Hands, a Virtual Emergency board meeting was called & budget for a DR in Dubai was approved by board members. The process to precure the DR setup started somewhere at the end of 2021. The major challenge during this time was Covid-19. Hardware unavailability was a concern as the silicon chips were extremely short because of mass colure of factories during Covid-19. The easy way would be to setup DR on a public cloud but it was against AAAID policies to setup DR on any Cloud, Considering the secretive nature of their financial documentation. Even with a lot of availability challenges, travel restrictions for DC experts from Sudan to travel to Dubai because of Covid-19, By mid to late 2022, the AAAID DR in Dubai was completed.

Civil War April 2023: In mid of April 2023, on a Saturday morning Sudan was shell shocked when clashes broke out between the Sudanese Armed Forces and their paramilitary Rapid Support Forces. These violent confrontations, primarily in Khartoum, intensified the crisis, displacing millions and resulting in mass civilian casualties.

AAAID despite having a DR in Dubai, never had a business continuity plan in place. With in few hours of war started the communication from Sudan to the rest of the world was lost. Electricity was cut down, Mobile towers were taken down. By the end of the day on Saturday it was clear that DR needs to activated by AAAID, but as I mentioned there was no business continuity plan in place. There was no one assigned the role to start the recovery process in case of Disaster. Moreover the sole person in Dubai office who was responsible to for DR was on annual leave in Sudan. When Dubai office IT team started recovery process, to their shock, they realized that there was a major error during the sizing of DR as the storage wasn't enough to recover all the servers.

Another core issue they figured out while recovering that replication was not working on some servers from last few months leading to loss of data for that specific period. With in few weeks of Civil war AAAID started the process to shift their employees from Sudan to UAE office. Another major setback was that most employees had desktop computers & their data was saved on those desktop. The backup of those desktop was setup in a server which was never replicated over to DR. But IT team was hopeful that the lost data will be recovered once the Civil war ends & Situation normalizes. Their hopes further received a shock when 4th week into the civil war a Rocket which was meant to hit another building hit the AAAID office in Khartoum leading to fire in entire building. It was later reported that the data center was on fire & whatever was remaining or survived the rocket impact, it was looted.

Mistakes & lessons from their Approach by AAAID:

1. Lack of a Business Continuity Plan (BCP)

- **Mistake**: Although AAAID had a DR setup, it lacked a comprehensive BCP to ensure smooth operation and recovery in case of a disaster. No Proper defined roles or a structured plan, there was no one assigned to initiate DR when disaster happened.
- **Lesson**: Without an established BCP a DR is not going to be helpful. Designate backup personnel who can initiate DR process if the primary person is unavailable, with each person well educated in DR protocols.

2. Policy Constraints Against Cloud-

Based Solutions

- **Mistake**: AAAID's policies against Public/Private cloud-based DR prevented the use of a more flexible and scalable solutions, which could have addressed hardware availability challenges during the COVID-19 pandemic.
- **Lesson**: While policies are necessary, they should be adaptable, especially in crisis scenarios. Consider Private or Hybrid DR solutions or assess the security capabilities of cloud providers to ensure the support critical functions if on-premises solutions are infeasible.

3. Insufficient DR Sizing and Capacity

- **Mistake**: The DR setup in UAE was undersized, leading to insufficient storage to recover all servers. This compromised the AAAID's ability to restore some of the critical data and functionality.
- **Lesson**: Perform a thorough assessment & sizing. Better analysis to ensure DR infrastructure can handle the full scale of services that are important for business continuity.

4. Replication and Data Management

- **Mistake**: Some servers had not been replicating data for months, resulting in significant data loss.
- **Lesson**: Implement continuous monitoring of replication processes and set up alerts to detect failures.

5. Data Storage on Desktop Computers Without Offsite Backup

- **Mistake**: Most if not all employees saved their data on desktop computers without a offsite backups, leading to data loss when these computers were destroyed or stolen.
- **Lesson**: Always ensure the Implementation of policies that encourage storing data on network drives that are regularly backed up to the DR site.

7. Failure to Regularly Test DR Capabilities

- **Mistake**: The issues with DR sizing and replication could have been identified earlier if regular DR testing had been conducted
- **Lesson**: Conduct regular DR testing, including end-to-end drills, to identify any weaknesses in infrastructure, personnel, or procedures. The management has to be blamed for this for not going for a DR solution back in 2019 when it was first identified. BCP & DR takes time to get mature.

8. Reliance on Physical Financial Documents and Lack of Digital Copies

- **Mistake**: As organization the AAAID stored critical financial contracts and documents only in paper form, resulting in the complete loss of these assets when the Khartoum office was destroyed. Without digital backups, these irreplaceable documents could not be recovered.
- **Lesson**: Digitize all critical documents, particularly financial contracts, and store them in a secure, redundant digital archive. Software solutions like Microsoft SharePoint or OpenText Documentum should be used in such cases to avoid such major loss of documentation.

IV. CONCLUSION

AAAID's Data center Disaster goes to show that despite spending a major chunk of amount on DR, the financial loss that caused because of some Major & some minor miss management caused a great loss. A comprehensive BCP coupled with regular testing and redundancy, having policies enough to adapt to situations that may not be correctly anticipated, are of prime importance. For any organization, DR and BCP need to be viewed as an ongoing evolution of processes subject to repeated re-visitation and reinforcement for resilience during crisis situations.

REFERENCES

[1] Business Continuity & Disaster Recovery by Susan Snedaker https://www.academia.edu/36447976/Business_Continuity_and_Disaster_Recovery_Planning_for_IT_Professionals?email_work_card=title

[2] Sudan War: https://www.cfr.org/global-conflict-tracker/conflict/power-struggle-sudan

[3] Case Study: First hand Witness of Events as a Employee of the Orgnization.