ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 3, pp: (133-136), Month: July - September 2023, Available at: www.researchpublish.com

Towards Data Availability during Disasters

[1]Jumana Al-Turairi, [2]Fahad Almutairi

Dhahran, The Kingdom of Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.8305758

Published Date: 31-August-2023

Abstract: **Business continuity provides the governance, risk, and compliance framework for managing and ensuring the continuity and recovery of IT services in the event of an incident or disaster. Service continuity process covers three main functions; Service Impact Assessments (SIA), IT services availability controls, and the drills and compliances. Required availability controls for critical systems such as disaster recovery and backup strategies play a vital role in ensuring the availability and continuity of businesses and organizations. This paper presents the best practices for disaster recovery, highlighting the importance of disaster recovery during emergencies, data backup solutions, testing, validation, and compliance related activities.**

Keywords: **Data Availability, Disaster Recovery, Backup, Critical Systems, Business Continuity, Service Continuity, Recovery Time Objective (RTO), Recovery Point Objective (RPO).**

I. INTRODUCTION

Information Technology (IT) plays a vital role in most organizations where critical IT systems outages may cause a significant financial loss. During incidents and disasters, rapid recovery and restoration require effective disaster recovery strategies and business continuity plans. The main purpose of business continuity and Disaster Recovery (DR) solutions is to protect the organization’s assets and ensure the continuity of critical operations and services during emergencies and disasters. Applying controls to identified critical systems will reduce the risk associated with critical systems interruptions. The primary objective for an organization’s business continuity strategies is to safeguard data from unauthorized access, archiving critical data, and implementing data protection measures. That can be achieved by replicating, archiving, and restoring critical data to have an accurate and sufficient system recovery with minimal impact to business operation.

II. IMPORTANCE OF CRITICAL DATA

Critical data refers to specific types of data that are deemed essential or crucial for the functioning, operations, or security of an organization. Critical data may include sensitive information such as personal data, customers or employee data, or any information that if compromised or lost, could have significant negative consequences. The impact and importance are the primarily base for data criticality. Service and data criticality are being classified and identified during the Service Impact Assessment (SIA) activity, where systems and applications are being evaluated to measure the service/data loss impact as well as service criticality. This covers multiple aspects such as: financial, reputation, business interruption, service criticality time, manual work-around procedures, health and safety etc. The result of the SIA will dictate the required availability controls such as sufficient backup, high availability, and disaster recovery solutions. Without comprehensive, reliable and accurate data, disaster management becomes more challenging; hindering efforts to recover and restore systems.

III. CAUSES FOR CRITICAL SYSTEMS OUTAGES

In today’s rapidly advancing technological world, it’s important to understand that different outages may require distinctly unique solutions. Data is the base layer that operations rely on. The aim of organizations is always to protect critical data from loss and threats by implementing effective business continuity, security controls, backup, and recovery strategies. The following are the main five critical data outages:

A. Human error

Human error refers to any systematic error by a human. Despite the advancements in automations, humans play a crucial role in operating and maintaining IT systems. The potential for mistakes is always present, where human errors like mistakenly deleting critical data, poor password handling etc., may have severe negative consequences, leading to systems failure, downtime, and financial losses. According to a 2018 IBM study, human error is one of the top three main causes of data breaches, along with criminal attacks and system glitches [1].

B. Cyber-attack

The significance of cybersecurity has grown exponentially. Incidents of cyber breaches may result in various adverse outcomes, such as data breaches, network failures, or even the complete shutdown of critical infrastructures. The impact of these breaches is not limited to financial losses; they also negatively impact the reputation of the organization where customers and stakeholders lose trust in the affected organization to protect their information. Organizations invest in the security and data protection through implementing policies and enforcing new security rules.

C. Natural Disaster

Refers to a sudden and extreme event caused by natural processes of earth such as fire, earthquake, or flood. Such events cause a threat not only to human lives and properties, they also have significant impact on the environment and infrastructure, which directly affects the data availability. This kind of risk is neither controllable nor avoidable. It’s crucial to prioritize disaster preparedness and mitigation strategies to minimize the impact of these events, ensure systems resiliency, and data availability.

D. Software Failure

Refers to the occurrence of unexpected or unintended systems behaviors or errors. Software failures may occur due to various reasons such as code error, compatibility issues, unauthorized system change etc. Such failures can result in a wide range of adverse effects extending beyond a single system. It can also affect other cascaded systems or networks.

E. Hardware failure

Refers to any interruption of a hardware component functioning to its designated specifications. Hardware failure can occur due to a variety of reasons such as aging equipment, overheating, or even manufacturing defects. Such failure may lead to downtime, data loss, and significant impact to business operations. It’s essential for an organization to have robust backup and recovery systems in place to minimize the effects of hardware failures and ensure business continuity.

It’s important for the organization to regularly assess and address these potential vulnerabilities to minimize the impact of such outages and ensure smooth operations. Additionally, implementing effective backup and recovery strategies can play a crucial role in minimizing the impact of system outages.

IV. INFORMATION TECHNOLOGY AVAILABILITY SOLUTIONS

In today’s technological world, businesses heavily rely on technology to conduct their operations. Unforeseen events can disrupt critical systems and result in significant business operation impact and financial loss. To mitigate the risk associated with the downtime, organizations implement IT availability solutions. These solutions are designed to ensure that IT systems remain accessible at all times and under any situation. The solutions encompass a range of strategies and technology that aims to minimize downtime, protect valuable resources, and maintain productivity even during incidents/disasters. This involves implementing redundant systems, backup and recovery mechanisms, and establishing robust disaster recovery plans.

A. High availability:

One of the key components of IT availability is the redundancy. By utilizing redundant systems or components, organizations can ensure that critical services can continue to operate even if one component fails. Redundancy can be achieved through techniques like clustering, virtualization, and load balancing.

B. Backup and Recovery:

Data backup and recovery is the process of creating and storing copies of data in a secure location so that they can be restored in the event of data loss or corruption. Backups can be created manually or automatically, and they can be stored on and off site. There are many different types of data backup and recovery solutions available. Some popular options include:

- Tape backup is a traditional and reliable method of data backup. Tapes are inexpensive and can store large amounts of data. Tapes can be slow to restore, and they are not as portable as other backup solutions.

- Disk backup is a more modern and versatile method of data backup. Disks are faster than tapes and can be more easily restored. Disks can be more expensive than tapes, and they can only store a limited amount of data.

- Cloud backup is a newer and increasingly popular method of data backup. Cloud backup solutions store data in remote data centres, which can be accessed from anywhere in the world. Cloud backup solutions are often more reliable than on-site backup solutions, and they can be easily scaled to meet the needs of growing businesses.

No matter which type of data backup and recovery solutions is being utilized, it is important to have a plan in place for regularly backing up critical data. This will help to protect the data from loss or corruption, and it will ensure that you can quickly restore your data in the event of a disaster.

C. Data Replication to DR Site

Data replication to the disaster recovery site is a critical process for organizations to ensure the continuity of critical business operations. It involves copying data from a primary site to a secondary site, which is typically in a different geographical area. The purpose of data replication is to create a synchronized and up-to-date version of the primary data, ensuring that in the event of a disaster or disruption at a primary site, the organization can quickly switch to the secondary site to continue critical operations seamlessly. The process is typically achieved through various replication technologies such as synchronous or asynchronous replication depend on the organization’s recovery point objective (RPO) and recovery time objective (RTO).

V. TESTING AND VALIDATION

Drills are valuable tool for testing and validating the effectiveness of IT systems. They can be used to simulate real-world events, such as power shutdowns and cyberattacks to see how the system and support staff respond. This can help to identify any systems weaknesses and ensure the readiness of IT support staff able to respond to any unexpected events. There are a variety of drills that can be used to test and validate IT systems. Some common types include:

A. Tabletop drill

These drills are usually conducted physically in a meeting room. Such a drill gathers the key participants around the table to discuss how to respond to an emergency or crisis situation. It is designed to test and evaluate an organization’s response during unexpected events.

B. Simulation drill

These drills are scenario based to mimic real incidents to test and evaluate the IT support staff’s preparedness, response, and coordination. By simulating different scenarios, organizations can identify strengths, weaknesses, and areas for improvements. Such drills require participants to play specific roles and follow predetermined procedures to effectively handle the simulated situation.

C. Live drill

These are real-time simulations of an emergency or incident where involved staff will practice and implement predefined steps to respond to an incident and recover the system efficiently.

Drills can also be used to test the procedures and processes that are in place for responding to incidents. This can help to ensure that everyone knows what to do in the event of an incident and that the response is coordinated and effective. By conducting drills, organizations can help to ensure that critical IT systems are effective and support staff are prepared to respond to any incidents that may occur.

VI. CONCLUSION

Availability of critical data is essential during emergencies such as disasters and incidents. It can be used to track the progress of the emergency, recover the system efficiently, and coordinate the response. Without comprehensive, reliable and accurate data, disaster management becomes more challenging, hindering efforts to recover and restore systems. By implementing robust and effective disaster recovery strategies, organizations can mitigate the risk of data loss, minimize downtime, and maintain business continuity during incidents and disasters.

REFERENCES

[1] 2018 Cost of a Data Breach Study, July 2018.

[2] X. Yin, J. Alonso, F. Machida, E. Andrade and K. Trivedi, "Availability Modeling and Analysis for Data Backup and Restore Operations", IEEE 31st Symposium on Reliable Distributed Systems, pp. 141-150, 2012.

[3] S. Hord, I. Pasternack, V. Streeg, M. Plumely and J. Hendrickson, high availability architecture and strategy.

[4] ISO 22301:2019 Security and resilience, Business continuity management system, Requirements Published October 2019