IJCSPUB.ORG ISSN : 2250-1770
IJCS PUBLICATION (IJCSPUB.ORG)
INTERNATIONAL JOURNAL OF CURRENT SCIENCE (IJCSPUB)
An International Open Access, Peer-reviewed, Refereed Journal

NETWORK DESIGN AND PLAN

Niravkumar Patel
Sr.Software Engineer
University of the Cumberland

Introduction

The Disaster Recovery Plan for Hitachi Vantara is designed for IT professionals operating complex and diverse systems, services, and applications that comprise its IT assets, procedures, and business processes (Kuroishi, 2021). It is designed to identify and describe the critical IT resources and business processes in the business. It can assist IT staff develop and maintain plans, budgets, and performance goals to allocate available resources to meet project objectives and deliverables. It provides management information for estimating a project and delivery dates, assessing completion and rescheduling, and providing staff with performance information on key performance indicators (Kuroishi, 2021). It is based on a system that includes multiple systems that support planning and execution activities in management information that provides key performance indicators and management reviews, and projections (Kuroishi, 2021). The management information also helps decision-making in the risk management process. This is useful as it identifies where risks are classified and links the risk classification with critical activities. The use of risk classification and necessary activities as a framework for risk mitigation helps the organization develop a well-integrated and comprehensive security posture for all the assets. It also provides an objective indicator of the effectiveness of the risk control processes. This approach is essential to prevent vulnerabilities or risks from being exploited by the enemy (Kuroishi, 2021).

The Disaster Recovery Plan for Hitachi Vantara combines the essential recovery steps and tools for business continuity and disaster recovery. It provides the means to integrate and maintain an integrated system to recover vital information critical to an organization. It provides a reliable means for the recovery

of documents, data, and other information systems. It is used in support of emergency response and other emergency action (Kuroishi, 2021). It is used for the initial communication of events and provides for the maintenance of communication channels. It enables data to be immediately accessible to authorized personnel. It minimizes the time required for communication between systems (Kuroishi, 2021).

Scope

An effective disaster recovery plan enables Hitachi to recover its data and assets after a disaster. To prepare their recovery plan, they should follow, identify critical resources.

Determine the impact of a disaster (Milanez et al., 2021). Determine the recovery time objective. Develop a recovery strategy for each necessary help. Develop a recovery site to restore data to use the recovery plan to rebuild their system. Business continuity recovery is an essential component of business continuity planning. It is also a critical part of disaster recovery planning. Business continuity is the ability of a business to continue normal operations after a disaster event (Milanez et al., 2021). Business continuity is dependent on the regular performance of the business activities. Business continuity is also affected by the availability of the company's IT systems.

Disaster Recovery Plan describes what should be done in the event of a disaster. Data Backup and Recovery Technology describes the use of backup and recovery technologies to restore data in the event of a disaster. Backup and Recovery Services describes the types of services used during a data backup and recovery. Recovery planning can help reduce the risk of the event occurring. The plan can also help prevent the problem from occurring in the first place (Milanez et al., 2021). The program should also provide business continuity for crucial business processes. Recovery strategies should cover the affected system and the business process affected by the disruption. After a disaster event, businesses can recover from it by performing various recovery techniques. These techniques are called business resumption. It helps organizations quickly restore the business environment after a disaster and recover important business information such as customer lists, sales receipts, and reports (Milanez etal., 2021). Companies need to develop a detailed plan for recovering lost and damaged data to use that data to recover their business processes in the event of a disaster (Milanez et al., 2021).

Business continuity planning for their organization is essential to implement when there is an imminent threat to system availability or new technology (Milanez et al., 2021). Business continuity planning may also be required when a disaster affects many people and critical business processes. A

business continuity plan helps organizations keep their systems up to date and is designed to be implemented promptly. The primary goal of a business continuity plan is to provide their organization with a long-term solution to a specific problem (Milanez et al., 2021).

Assumptions

The system hardware and software configuration and security architecture in Hitachi is described using an enterprise architecture plan. The server, client, and application systems are described utilizing an enterprise architecture plan. The system configuration includes the hardware, its configuration controls, and its dependencies and components. The client configuration consists of the operating system, configuration controls, and dependencies and features (Milanez et al., 2021). The application configuration includes the applications, their dependencies, and their members. The system hardware and software are all considered to be vulnerable when considering the possibility of a disaster. The data may contain information about vital business functions protected by the IT system, which may also become data in an insecure manner or may have information integrity issues. The recovery time objective RTO is a cost-benefit ratio established by the organization after identifying all the potential disaster recovery points and assessing the time it would take to completely restore the system to its normal state or restore partial or all functionality of the system (Milanez et al., 2021). The assumptions are made based on the physical and logical conditions of the system. These conditions may change in the event of a disaster. Hardware is defined to enable an entity to function effectively or meet a business environment's needs. Software is an integrated application component that runs on a computer or a mobile device. Data are the raw, unstructured information stored by a system. The plan includes assumptions about the following system hardware, applications, and data. The program also includes specific time and project management instructions and a template for future planning exercises. The project manager is required to evaluate the overall plan and revise the program based on their evaluation (Milanez et al., 2021).

Incident Commander

The Incident Commander is responsible for managing the overall disaster recovery program and directing the recovery efforts daily (Putra, 2021). The Business Recovery Manager is responsible for developing the business recovery plan. This individual controls all aspects of the program, including choosing the teams, determining who will receive supplies, organizing travel to the disaster site. The Incident Commander, who has the same responsibilities as the disaster recovery manager, focuses on

ensuring that the recovery of the business continuity plan is a success (Putra, 2021). The Commander coordinates the efforts of all company functional areas, such as finance, operations, and security, to fulfill the business continuity requirement. The disaster recovery coordinator is the last person to be seriously affected by a disaster. In this role, the coordinator briefs senior management, members of the company's board of directors, and the CEO on the critical strategic issues. In addition, the coordinator ensures that strategic planning and critical business decisions are communicated to the appropriate stakeholders. The incident commander ensures that resources are available and coordinating all the recovery steps with the disaster recovery coordinator. The incident commander ensures no disruptions to service due to the disaster recovery plan (Wallace & Webber, 2018).

Incident Command Team

The Incident Command team leader directs all operations and maintains communication with the other plan members (Putra, 2021). The primary role of the team leader is to coordinate recovery activities between all the recovery teams. The team leader also controls the plan's day- to-day operations, such as issuing and updating procedures and dispatching equipment and resources. The person in charge of the planning and implementing a project is the Disaster recovery, the plan administrator. The person responsible for developing and maintaining an effective disaster recovery plan is the disaster recovery plan's coordinator. Each team is responsible for developing its specific areas of responsibility. Once a project is established, the team members will work closely to ensure its effectiveness (Putra, 2021). The team members must be knowledgeable about their area of responsibility and have the necessary resources to perform their duties. The primary team member is the incident commander, and the second member is an assistant. The incident commander is usually the IT technical team leader. The assistant ensures that the plan is executed, documenting the project, keeping records of all actions taken, and updating team members when needed. The Disaster recovery manager is responsible for developing the disaster recovery plan and directing and coordinating all team activities. The Disaster Recovery team members are responsible for reporting the incident to the appropriate authorities, conducting damage assessment, providing first aid, initiating the recovery process, and managing personnel until the situation is stabilized and the public safety situation is under control (Wallace & Webber, 2018).

Data Recovery Information

The Hitachi Vantara disaster recovery system can be used to create a consolidated data recovery data warehouse. It enables a company to quickly store a complete set of damaged data from different sources (Rosas et al., 2021). When disaster recovery is needed, it can restore data to a particular point in time at the most appropriate level for data accuracy and speed. The major benefit of the Hitachi Disaster Recovery is that it can recover in real-time in any geographic location. This program is designed to create an automated backup system for all data in the organization. It does this by creating a temporary backup file each time a critical process is changed. This file is created, verified, and saved in the organization's data backup location. It can also use the file to recover a system backup if the system is affected by a security incident (Rosas et al., 2021).

A virtual recovery solution stores a replicated copy of the operating system and all other data in a remote data center (Rosas et al., 2021). The primary data recovery process is required to provide an automated backup and restore all data and information. It also helps restore data if the primary data center fails and only the backup data are available at the alternate site. The backup data is always stored in a separate file for all three business units. The backup and restore process involves a combination of disk and tape backup. It does not just include the traditional file backup as it does not save data in a single file. Each file's backup and recovery time are stored separately in the tape library and can be retrieved by any compatible backup software. A multiuser system is a collection of computers in a network that is used to store files. These are used synchronously and asynchronously (Rosas et al., 2021).

Conclusion

In a disaster recovery plan in Hitachi Vantara, the IT experts of the organization first have to meet face to face to discuss the disaster recovery issues related to their organization. They cannot communicate with each other, and therefore the IT experts must establish a working team without contacting each other (Rosas et al., 2021). The IT experts of the organization prepare technical specifications on the system in which they are working and use these specifications to prepare training materials about the plan for their use. The IT professionals are responsible for training the team on the IT processes and procedures that should be followed in the actual work on the system. The IT professionals in Hitachi are accountable for developing the recovery procedures based on the information gathered during the planning process (Rosas

et al., 2021). The organization is always on the alert for unusual or unusual incidents that may lead to a disaster. For example, a fire at a warehouse or an earthquake might interrupt electrical power, rendering the building uninhabitable. The disaster recovery team has to ensure that the power back on is quickly restored. The system recovery planning in Hitachi Vantara is based on the expertise of the recovery team members, on the knowledge of the disaster recovery professionals, on the expertise of the management of the disaster recovery process, and on the involvement of the stakeholders, who have been identified in the disaster recovery planning process (Rosas et al., 2021).

References

Kuroishi, I. (2021). Social Resilience in Disaster Recovery Planning for Fishing Port Cities: A Comparative Study of Prewar and Twenty-First-Century Tsunami Recovery Planning in the Northern Part of Japan. Journal of Urban History, 47(2), 332-353.

Milanez, B., Ali, S. H., & de Oliveira, J. A. P. (2021). Mapping industrial disaster recovery: Lessons from mining dam failures in Brazil. The Extractive Industries and Society, 8(2), 100900.

Putra, R. A. B. N. (2021). Strategic Recovery Plan: The Resilience of Wyndham Garden Kuta Beach Bali after Major Impacts of Covid-19 Pandemic. International Journal of Glocal Tourism, 2(1), 13-27.

Rosas, E., Roberts, P., Lauland, A., Gutierrez, I., & Nunez-Neto, B. (2021). Assessing the Impact of Municipal Government Capacity on Recovery from Hurricane Maria in Puerto Rico. International Journal of Disaster Risk Reduction, 102340.

Wallace, M., & Webber, L. (2018). The disaster recovery handbook: a step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets. New York, NY: AMACOM. ISBN-13: 978-0814438763