Riptide Analytics – Disaster Recovery and Business Continuity Plan

Kristine Plunkett

March 7, 2021

Table of Contents

Riptide Analytics – Disaster Recovery and Business Continuity Plan

The world is full of imminent threats, potential disasters, and situations that an organization must plan for, even better yet, mitigate. These risks can be anything from burst water pipes, blizzards, earthquakes, hurricanes, fires, cyberattacks, or even terrorist attacks that have potential to impact operations (Cascardo, 2020). Disaster recovery planning has been defined and interpreted by many in various ways such as the developing of a written plan to address the process by which an organization will continue to conduct business in instances of interruptions. In addition, it has also been described simply as a plan of action, or alternatively an integral component of resource management (Bandyopadhyay, 2001). The underlying meaning of disaster recovery planning within this exercise will be stated as the planning, documentation, and continued maintenance efforts involved to ensure the continuance of business functions and capability to recover all assets in a timely and orderly fashion in the event of disaster or outage.

Riptide Analytics, LLC, is a company specializing in providing data analytics solutions to the vineyard and wine distribution industry through cloud-based software-as-a-service solutions and applications. Located in Central California, the organization is uniquely susceptible to the impacts and dangers that large magnitude earthquakes in this region can inflict. In addition to earthquakes, the region where the facility is located is uniquely vulnerable to wildfires, especially troublesome in years following severe drought in the State. As such, it is pertinent that Riptide Analytics, LLC invests in and composes a thorough disaster recovery and business continuity plan in efforts to ensure the continuance of technical systems and business operations in times of disaster. Following will detail the disaster recovery and business continuity planning efforts that Riptide Analytics, LLC will need to implement in order to ensure mitigation and recovery from disasters runs smooth, is easily understood, and easily initiated.

Policy Statement

The Riptide Analytics LLC executive leadership team have approved and set aside financial and workforce assets in order to design and develop a companywide disaster recovery plan. This disaster recovery plan will entail all aspects of disaster recovery that will include a requirements gathering phase, in addition to setting clear-cut recovery objectives. The risks involved will be highlighted in a risk assessment, which will document any infrastructure, systems, networks, and cloud assets that must be protected from outages and/or disaster. The employees of Riptide Analytics must also be made aware of, and participate in, the disaster recovery planning, testing, augmentation, and initiation efforts.

Purpose

The purpose of this document is to outline the disaster recovery planning steps that will be created and maintained for Riptide Analytics, LLC. The general goal is to ensure that all operational functions and technology are protected from threats, outages, and disasters with very little acceptability of downtime. This is especially true for all client facing applications and solutions that are hosted in the cloud. In addition, it is imperative that the facility and the employees that work within them are kept as safe as possible, and aware of how to activate the disaster recovery plan and what steps will need to be taken to reach full recovery.

Scope

Riptide Analytics, LLC is a single state, single site business that heavily relies upon cloud-based systems for the internal technology as well as for Software-as-a-Service solutions for the customer base. These cloud-based systems are hosted within the Amazon AWS datacenters located in the San Francisco, just 3 hours north of the Riptide Analytics headquarters. The headquarters facility is the sole site of the organization, that which will be detailed within this

disaster recovery plan document. The facility is located in the small coastal town of Harmony, San Luis Obispo County, California. This document will outline the risks involved for Riptide Analytics, LLC, in addition to mitigation steps and documentation of what to do in case of disaster or an outage at the facilities.

Objectives

The main objective of this disaster recovery plan will be to design, develop, test, document, and continually improve upon a well-orchestrated and easily initiated disaster recovery and business continuity plan. The ultimate goal will be to mitigate risks where possible, and provide for solid plans for recovery of information technology assets and business functions. It will be necessary to ensure that employees know what to do if or when a disaster should strike, anything from a power outage to a large magnitude earthquakes or fire will be well addressed.

Assumptions

There are many assumptions that must be made throughout these efforts. First and foremost, it is assumed that the facility of Riptide Analytics is built to code and capable of withstanding moderate to severe earthquakes. Therefore, the issue will be the recovery and continuation of business operations in the event of severe large scale magnitude quakes, which have plagued the State of California for many years. Also, there should be consideration for a total facility loss in the case of wildfire, whereby if possible a mirror site will be necessary to mitigate this risk.

Asset Inventory

The main assets of Riptide Analytics, LLC will be the headquarter facility in Harmony, CA and any technology that is maintained there. The goal initially when Riptide Analytics was created was to ensure organizational resilience and business continuity, the executive leadership

teams coming from technology backgrounds, were adamant that securely configured cloud services were the way forward in business and removed the need for extensive IT teams to manage systems and software on-sight. All development and production environments are hosted on AWS cloud infrastructure. All staff are well prepared with laptops and mobile phones to be able to work on the go when necessary, at times some already working from their homes. Data is stored in the cloud on private servers and data encryption at rest has been activated for all data to ensure the integrity of industry trade secrets and intellectual property.

The backend of the cloud infrastructure of Riptide Analytics was designed in such a way as to provide for incredible resilience with zero downtime for the client facing data analytics applications and solutions. The main applications are hosted only 3 hours away in one of the datacenters located in San Francisco, CA. Should a large magnitude earthquake severely impact the headquarters in addition to the AWS datacenters in San Francisco there is a mirrored site in the Seattle, WA datacenter. There are also backups of the system configurations and data that are replicated nightly to a datacenter in Virginia, and one overseas in Dublin, Ireland. It would take total destruction of transatlantic communication cables, or a disastrous event of monumental proportions and beyond imagination to take down the client facing solutions of Riptide Analytics, LLC.

Risk Assessment

The risk assessment has highlighted areas where risks exist and could be benefited through mitigation efforts. A risk matrix was created in order to ensure all risks are documented and their corresponding risk scores detailed so as to help in prioritization exercises. Restoration of client facing services has been deemed urgent and of top priority. This is easily accomplished through the AWS console, checking for uptime effects and impact to datacenters. Any issues

witnessed, the development team has been made aware to script the systems over to utilize a separate datacenter. Alternatively, this process is also configured with advanced load sharing and distribution techniques, automatically changing servers if there is downtime or latency being logged.

Outside of securing the main client facing SaaS product of Riptide Analytics, there are many operational applications in use by the differing business units. The good news is that these applications are also solely cloud based, however many of which are supplied by outside vendors. In this case, it has been decided that ensuring the sales and marketing teams, in addition to support functions, are all brought online as soon as possible.

The Recovery Time Objectives for these business units have been set to 1 hour. Contractual agreements with these vendors promise 30 minutes, so this should be entirely feasible. Discussions have taken place with outside vendors and all have similar backend architecture in the cloud as Riptide's, therefore downtime will be optimistically limited. Finally, the finance and accounting business unit is rather exposed running legacy accounting software on the controller's laptop. It is backed up to AWS S3 cloud storage, however the recovery time will be greater than that of other services, which has been agreed to be acceptable.

Cloud Based Risk Mitigation

Advancements in technology, specifically cloud based solutions, have enabled organizations to build resilient organizational structures capable of mitigating even some of the most deadly of risks (Jasgur, 2019). The ability to run mirrored sites in differing geographical locations is astounding and has truly revolutionized disaster recovery planning, however there are a great many risks that need to be addressed to ensure this resiliency.

First off, securing the systems and applications is entirely essential. Utilizing cloud based solutions for disaster recovery efforts can prove cost effective, especially true when taking advantage of the public cloud, a method of pooling technology resources that are consequently shared among multiple organizations (Trovato, et. al., 2019). This benefit is easily diminished in seconds should a data breach occur and sensitive customer data consequently compromised. In addition, trust can be an issue with cloud based systems, as can security and control of data when utilizing cloud based solutions (Lee and Brink, 2020). For these reasons, the risk mitigation strategy of Riptide Analytics, LLC has been to utilize the private cloud, meaning the back end infrastructure in the datacenter at AWS is solely in use only by Riptide Analytics. These applications and solutions run on their own servers and data pipelines to ensure the upmost security and integrity of information. In addition, the use of Amazon's EC2 instance store encryption is in place, which will ensure even the strictest of regulatory compliance frameworks for stored data (AWS, 2021). Finally, the executive leadership of Riptide Analytics has contracted AWS experts to frequently consult on setup and configuration endeavors to ensure that the systems are maintained to the highest standards and not exposed to vulnerabilities.

Damage Assessment

The emergency operating center will be located at the CEO's ranch house 14 minutes south of the facility and all recovery efforts will be capable of taking place from this location. The ranch includes a bunker that is capable of withstanding local wildfires and earthquakes of biblical proportions. Data and communications equipment enters the facility through high powered T1 connections, alternatively there are military grade satellite communication backups. The bunker is a fully equipped emergency operations center, capable of maintaining the organization of Riptide Analytics, LLC and all staff for a minimum of six months. This is

extremely effective for tackling even a complete structure devastation of the Riptide Analytics headquarter facility due to potential wildfire impact in the region.

In the case of a severe magnitude earthquake, once all staff have safely evacuated the premises, the facilities team will conduct a damage assessment of the structure once it has been deemed safe to re-enter. Post disaster damage assessment studies of the Paso Robles earthquake highlighted the fact that much of the workforce interviewed for the study were in their offices at the time the quake struck (McEntire, et. al., 2012). It was uncovered that most of the employees went outside and witnessed the severe damage within the surrounding areas and collapsed buildings before a formal response to the disaster took place.

Ultimately, every step has been taken to secure the resilience of the organization, systems, infrastructure and data. The safety of the employees is the top priority, therefore a semi-annual safety and evacuation exercise has been in place to ensure all are aware of what to do when disaster strikes. Once loss of life has been protected, it is then pertinent to move onto the next step by expediting the initiation of the disaster recovery plan, and assess damage of facility and systems to commence moving toward recovery efforts efficiently.

Activation Criteria

Earthquakes historically plague the region known as the ‘ring of fire’ that encompasses most all of the rim of the Pacific Ocean, including East Asia, coastal Alaska, and the western seaboard of the United States (Chen, et. al., 2020). Riptide Analytics, being located in Harmony, CA, directly situated along the Pacific Coast, is extremely vulnerable to the impacts of a large scale earthquakes. Therefore, the main criteria that will initiate this disaster recovery plan will include loss of power or communications at the Riptide Analytics facility, potential flooding of the facility due to burst water pipes, potential impact from local wildfires, large magnitude

earthquakes, or other unforeseen disasters that have potential to disrupt business operations or communications.

Delegation of Authority

The delegation of authority delineates the direct succession from executive leadership through top management teams of each business unit. Succession planning within the organization at Riptide Analytics has taken place, which would be suitable even under the strictest of publicly traded organizations. The human resources team have been very detailed in documenting those of the workforce who are capable of taking on the duties and responsibilities of senior managers with frequent exercises on knowledge share and briefings taking place (Tucker, 2015). The delegation of authority has been approached as it would be even for any governmental entity, the planning and succession training taken extremely seriously. It has been adamantly instilled in the workforce that they are to take action to respond to disasters and thoroughly understand their duties to take on authority for these efforts when necessary.

Continuity Organizational Structure

The organizational structure at Riptide Analytics will closely resemble that of the typical day to day organizational structure. Top executive leadership consists of CEO, CFO, and CIO, under that the top senior managers within their respective reporting bodies. Each senior manager also has performed succession planning within their teams, maintaining no less than two staff members capable of stepping up and taking ownership and responsibility.

Ops and Communication Protocols

As discussed, the emergency operations location will be located at the CEO's ranch house bunker compound, just minutes south of the facility. This bunker is ideal with its ability to withstand incredible disasters and still maintain communications. Emergency contact information

is created and stored in multiple locations onsite and in the cloud, accessible to all staff. This information includes both internal personnel and outside vendor contact information for all contractors and vendors that work with or provide infrastructure and systems for the organization. Additionally, an online social platform is available for the Riptide Analytics team to internally communicate and a separate channel is available to communicate with vendors and the customer base. This will enable the relay of information in a broadcast methodology instilling confidence and assurance to the customer base that the team at Riptide are aware of any issues that may be occurring at present and assure that these are being addressed.

Recovery Objectives

Recovery point objectives and the maximum allowable time for outages were thoroughly discussed and agreed upon in efforts to align the critical business functions and resources that must be recovered and made available after experiencing a disaster (Tucker, 2015). As outlined above, the recovery point objectives for customer facing solutions will be within minutes of a disaster taking place. Regarding all 3rd party vendor provided cloud solutions the recovery point timeframe is contractually agreed upon to be within 30 minutes. Finally, the finance and account solution is to be brought back online within 3 – 5 hours. This business unit will be able to help with operational recovery efforts and bringing the team online at the CEO's ranch house bunker, and also this realistically grants tech teams time to restore finance systems and data.

Testing Protocols

Testing is as crucial as planning when it comes to disaster recovery and business continuity endeavors. The ongoing testing scheduling should take place at least every six months to ensure that all employees, infrastructure, and technology are kept up to date and accounted for within the documents and planning efforts. Advancements in technology are extremely fast

paced, therefore it is imperative to ensure that the latest updates of technology in use within Riptide Analytics are updated frequently within this disaster recovery plan so that it is regularly maintained and up to date. In addition, it is important to regularly update any contact information for employee's, vendors, and clients as soon as they have changed in order to maintain flawless communication efforts.

Continued Maintenance

The disaster recovery plan will need to be tested regularly and alterations made as circumstances at the facility, with emergency contacts, technology updates or changes, essentially anything that can alter the way the plan will function or what the plan will cover. Any changes within the working environments, technology added or removed, in addition to employee data must continue to be visited frequently to address continued maintenance concerns.

Confidentiality

Finally, it is imperative to address the confidential nature of this disaster recovery plan. Confidentiality of the disaster recovery plan needs to be maintained with the strictest of secrecy. This plan entails industry trade secrets, sensitive data and systems information that enables Riptide Analytics, LLC to maintain a competitive edge in an extremely competitive marketplace. The human resources team have engaged to ensure that all staff at Riptide Analytics, LLC have regularly updated and signed non-disclosure agreements and statements to the confidential nature being maintained for all disaster recovery and business continuity information and documents.

References

AWS. (2021). *How to protect data at rest with Amazon EC2 instance store encryption*. Retrieved from https://aws.amazon.com/blogs/security/how-to-protect-data-at-rest-with-amazon-ec2-instance-store-encryption/

Bandyopadhyay, K. (2001). The Role of Business Impact Analysis and Testing in Disaster Recovery Planning by Health Maintenance Organizations. *Hospital Topics*, *79*(1), 16.

Cascardo D. (2020). Learning to live with Volatility: Preparing for business continuity and recovery following a disaster. *Physician Leadership Journal. 7*(4):69-72.

Chen, T., Chao, T., and Cheng, H. (2020). Exploring the changes in risk perceptions and adaptation behaviors based on various socioeconomic characteristics before and after earthquake disasters – A case study in Taiwan. *Natural Hazards and Earth System Sciences, 20*(9), 2433-2446.

Jasgur, C. (2019). Leveraging disaster recovery in the cloud as a cloud migration path: A case study. *Journal of Business Continuity & Emergency Planning*, *13*(2), 150–159.

Lee, L. S., & Brink, W. D. (2020). Trust in Cloud-Based Services: A Framework for Consumer Adoption of Software as a Service. *Journal of Information Systems*, *34*(2), 65–85.

McEntire, D., Souza, J., Collins, M., Peters, E., & Sadiq, A.-A. (2012). An introspective glance into damage assessment: challenges and lessons learned from the Paso Robles (San Simeon) earthquake. *Natural Hazards, 61*(3), 1389–1409.

Trovato, F., Sharp, A., & Siman, T. (2019). Cloud, co-location, on-premises and hybrid disaster recovery solutions: Pros, cons, and a cost comparison. *Journal of Business Continuity & Emergency Planning*, *13*(2), 120–135.

Tucker, E. (2015). *Business continuity from preparedness to recovery: A standard-based*

approach. Waltham, MA: Elsevier.