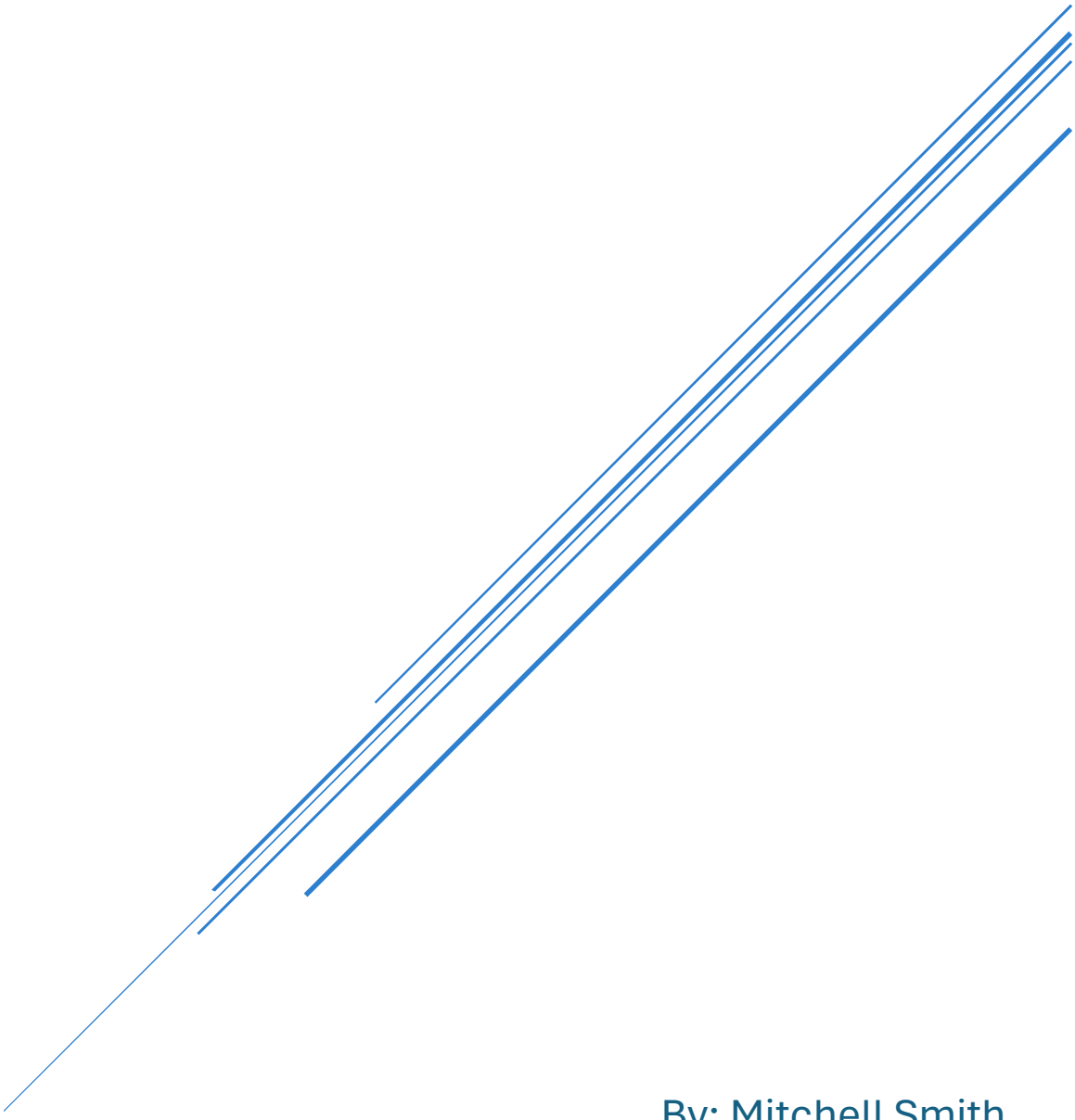
ASSIGNMENT #4

DBAS3080



By: Mitchell Smith
W0440925

Table of Contents

Introduction

In this document, I will demonstrate the completion of the assignment requirements by conducting research on a company of my choosing and identifying factors that could influence their disaster recovery operations, identifying their regulatory bodies and compliance challenges that are associated, creating disaster recovery, backup, and business continuity plans for the company, and receiving feedback from a classmate regarding the plans that I created.

Task 1: Disaster Recovery Policies & Regulatory Body Compliance

Assignment Questions and/or Required Screenshots Provided Below.

OBJECTIVE #1. Identify formal policies, processes and people that influence Disaster Recovery in a company of your choosing.

Company:

The company that I am going to focus in on for this question will be the company *"Microsoft"* which is one of the largest technology companies in the world that offers an extremely wide variety of services to consumers, such as cloud computing services (Microsoft Azure), computing hardware and OS (Windows), company / education services (ex. Microsoft Word, Microsoft Teams, Microsoft Excel), gaming hardware (Xbox) and more.

Policies:

Microsoft has established the "Enterprise Resilience and Crisis Management" (ERCM) policy, which consists of strict requirements for disaster recovery plans that have been created and established by the company to undergo extensive annual reviews that include in-depth testing and analysis of the plan to ensure that it meets company standards, implementation of updated operations / technology to the plan to improve the outdated aspects that were discovered during the testing / analysis of the disaster recovery plan, and extensive reviews of disaster recovery plan documentation to validate and complete each annual review. Additionally, the ERCM policy requires that after action reports of each review must be created that outline the outcome of each disaster recovery plan review, the actions that were taken throughout the review, and the changes that were made to the plan throughout the review.

Processes:

The ERCM policy requires that the Microsoft ERCM team must conduct extensive testing during their disaster recovery plan reviews that consists of a variety of scenarios that could have a major impact on the company, such as scenarios that impact people, locations, and technology. Each testing scenario has a specific threshold of requirements / criteria that must be met for each testing scenario to be validated and established by the company, with certain testing scenarios having a greater number of requirements / criteria to meet than others due to the severity of impact each individual scenario could have on the company. These types of testing / processes are put into place for the purpose of addressing a large scale of threats to the company. After the extensive testing has been completed, disaster recovery documentation must be thoroughly reviewed to ensure complete accuracy throughout the entirety of the plan, as well as clear implementation of new processes / technology that were integrated into the plan. After action reports must also be created to outline the results of each review and all the steps that were taken to follow the ERCM policy throughout the course of the disaster recovery plan review.

People:

Microsoft has assembled a team of IT specialists that they label as the Enterprise Resilience and Crisis Management (ERCM) team. This team is directly responsible for the management of disaster recovery operations for all Microsoft platforms / services, including the creation of disaster recovery plans within the company.

OBJECTIVE #2. Identify specific Regulatory Bodies and the major compliance challenges they present to the company. Highlight any compliance regulations that you do easily or well.

Due to the company Microsoft being an international tech giant, the company is governed by several regulatory bodies. Because of this, I am going to focus in on the regulatory bodies that govern Microsoft in Canada and Europe.

Canada

In Canada, the regulatory body that would govern Microsoft would be the Federal Government of Canada due to the federal laws that Microsoft and other tech companies must abide by. These laws are as follows:

Consumer Privacy Protection Act (CPPA) – Governs the possession and usage of Canadian's personal data that is collected and utilized by businesses.

Personal Information and Electronic Documents Act (PIPEDA) – The original data privacy act that was made into law in 2001 and governs the possession, usage, and distribution of Canadian's personal data by businesses.

Compliance Challenges – The PIPEDA and CPPA law contain heavy regulations for how an individual's data is stored, handled, and distributed by companies / businesses across Canada and carry significant fines if these regulations are not followed, such as businesses being issues fines of up to $10,000,000 or 3% of their gross global revenue. Under the CPPA, all companies that possess an individual's personal data also must create their own privacy management program and distribute this information to the government of Canada immediately upon request. Businesses are also required under the federal laws to implement mandatory data security practices to ensure that individuals' data is being correctly safeguarded. Finally, there are regulations that require clear and valid consent to be obtained from an individual when obtaining their personal data and there are also data breach notification regulations that require data breaches to be reported to the privacy commissioner.

Europe

EU general data protection regulation (GDPR) – In Europe, Microsoft is primarily governed by the European Union, the European Commission, and the European Data Protection Board through the EU general data protection regulation (GDPR), which establishes the rights of an individual's personal data and how it is stored and utilized by companies.

Compliance Challenges – The GDPR law presents major compliance challenges to all tech companies in general due to their strict regulations in terms of how an individual's data is handled, distributed, and protected by businesses. It is even recommended on the Council of the European Unions website for businesses that handle individuals' personal data to appoint a data protection officer to ensure that companies are all in full compliance with the GDPR. The GDPR also contains strict regulations pertaining to the distribution of an individual's data and especially when distributing that data to non-EU countries. Finally, there are strict data breach notification laws in place under the GDPR if businesses suffer a data breach incident.

Task 2: Disaster Recovery, Backup, & Business Continuity Plans

Assignment Questions and/or Required Screenshots Provided Below.

OBJECTIVE #1. Create a disaster recovery, backup, and Business Continuity plan for the company.

Disaster Recovery Plan

The disaster Recovery Plan that I would implement for Microsoft would consist of the following steps:

Step 1. To properly follow the ERCM policy that governs disaster recovery plans, we would first need to conduct multiple test scenarios to determine the scale of potential threats to the company that the disaster recovery plan needs to address. This will help the Microsoft to determine which threats need to be more focused on than others due to the different levels of severity that each threat poses.

Step 2. After we identify the threats that Microsoft could potentially be faced with, we then need to analyze and identify what specific outcomes of the disaster recovery plan need to be prioritized. Given that Microsoft is one of the biggest technology companies in the world currently, I would imagine that they possess tons of crucial data that needs to be safeguarded at the highest level. I also would think that whereas Microsoft possesses data centers across the world that are critical to their daily operations, mitigating their system downtime in a disaster situation would be another top priority of the company.

Step 3. Now that we have identified our main priorities of our disaster recovery plan, we then need to define a Recovery Point Objective (RPO), which is basically a threshold of what kind of data loss can be tolerated by the company and what kind of data loss poses a major risk to the company and must be recovered in the event of a disaster situation.

Step 4. Now that we have defined an RPO to account for the threshold of what kind of data loss is and is not acceptable, we also need to create a Recovery Time Objective (RTO) to establish a threshold for how long their critical data center systems can suffer downtime before it begins to pose major risks to the company.

Step 5. Next, we need to establish and create a contact list for the group of employees / external parties that will respond to disaster situations when they occur for the purpose of prioritizing communication and efficiency in DRP responses.

Step 6. Now that we have laid the foundation for what problems we are addressing, what our priorities are, what our RPO/RTO is, and who will be responding to a disaster situation, we now must develop effective strategies to combat all types of disaster situations that may occur.

Step 7. Throughout the entirety of this process, we should be creating in-depth documentation of all aspects of the disaster recovery plan, as well as After action reports (per ERCM policy requirements) that outline the results of each review and must be reviewed by the ERCM team before it can be validated and established as an official backup plan.

Step 8. To align with the ERCM policy requirements, this disaster recovery plan will be extensively tested and reviewed at least every 12 months. Regularly reviewing the DRP documents will help to determine whether any changes or updates could be made to the DRP procedure to improve the effectiveness and efficiency of the DRP response operation, and it will enhance the efficiency of the operations by giving the response personnel practice in their roles in the event of a real DRP response.

Backup Plan

Due to Microsoft being one of the worlds largest tech companies, this means that they inevitably possess extremely large amounts of data that is stored and utilized daily to run their company. Because of this reason, both hot and cold backup strategies must be integrated to ensure that their crucial data is being constantly backed up using multiple different backup methods and technology, which will play a fundamental role in safeguarding the company's crucial data at the highest level. The backup strategies that I would deploy for the company are as follows:

Hot Backup Strategy

Step 1. Schedule time periods for each type of backup procedures that will be utilized by the company to be conducted while the server(s)/system(s) remain active.

Step 2. Implement backup monitoring and backup report software that will automatically monitor the performance of the backup procedures and create reports of the results.

Step 3. Implement data encryption methods as a layer of security while crucial data is being backed up (precautionary measure).

Step 4. Deploy load balancing software to ensure that crucial data can be efficiently backed up while company servers remain active.

Step 5. Automated incremental backup procedures should be integrated to back up crucial data to an off-site external environment on a daily basis. This will help to ensure that crucial data is consistently being updated.

Step 6. Data replication software should be integrated as a daily method that will ensure an additional set of data is being stored in an external environment that is consistently updated and accurate.

Step 7. Automated differential backups should be integrated and utilized 2-3 times per week to store updated versions of the data since the last full backup occurred to an external environment.

Step 8. Consistently review, test, and document the backup plan to ensure that up-to-date versions of company data is efficiently being copied without disrupting server/system operations. This will allow for possible improvements to be made to the plan in the future if needed. Backup procedures should be thoroughly tested at least every 3 months.

Cold Backup Strategy

Step 1. Implement backup monitoring and backup report software that will automatically monitor the performance of the backup procedures and create reports of the results.

Step 2. Implement data encryption methods as a layer of security while crucial data is being backed up (precautionary measure).

Step 3. Schedule time periods when the server(s)/system(s) are offline to conduct backup operations.

Step 4. Perform full backup procedures while the server(s)/system(s) are offline to create replicas of all company data.

Step 5. Follow the 3-2-1 backup rule and store two additional copies of the data on two different types of media devices and have one of those copies stored away from the workplace.

Step 6. Consistently review, test, and document the backup plan to ensure that up-to-date versions of company data are consistently being copied and stored. This will allow for possible improvements to be made to the plan in the future if needed. Backup procedures should be thoroughly tested at least every 3 months.

Business Continuity Plan

The business continuity plan (BCP) that I would create for the company “Microsoft” would consist of the following steps:

Step 1. To begin, we must analyze which services are critical to the operation of the company, even while dealing with a disaster situation. This will help us to determine which methods need to be created for specific services to maintain the crucial functionality of the company while a disaster situation is in progress and a disaster recovery plan has been initiated to deal with it. In terms of Microsoft, critical services that must be maintained could include Microsoft Azure and Microsoft 365 due to the services being fundamental / critical to the operations of businesses and educational purposes.

Step 2. Next, we must conduct a risk assessment to understand what the results / impact will be of eliminating services that are not fundamental / crucial to the operations of the company. Certain services being temporarily eliminated due to being non-essential could still mean that the company could suffer financial impacts, overall dissatisfaction from customers etc.

Step 3. After analyzing and identifying the services that must remain functional in a disaster situation, we then need to develop strategies for each critical service to ensure the consistent functionality of all critical services when a disaster situation presents itself. An example of strategies that could be created / developed could include utilizing backup servers through integrating redundancy and failover mechanisms.

Step 4. After we have developed effective strategies to maintain crucial functionality of the company during a disaster situation, we must then create an emergency preparedness team, which is a group of employees within the organization that will be trained to respond to specific aspects of the business continuity plan in a disaster situation and ensure that the methods to maintain critical services have been deployed. The number of staff that will be integrated into the emergency preparedness team will be dependant on the amount of expertise that will be required to effectively maintain the functionality of the company's critical services. Some examples of the roles that staff members would be appointed could include Crisis and incident Managers, Business Continuity Managers, Business Continuity Specialists, Crisis Intervention Specialists, and IT Recovery Technicians.

Step 5. Once a rough draft of the business continuity plan has been created, the emergency preparedness team that has been assembled must review the documentation to understand their individual roles and responsibilities when a disaster situation presents itself and the business continuity plan must be initiated. This will help to identify which specific aspects of the plan will require certain members of the team to undergo training.

Step 6. The business continuity plan must be thoroughly tested and validated before becoming established as the official plan. Regular reviews must be conducted once the

plan has been established to ensure that the plan is as effective as possible and that no updates need to be made to certain aspects of the plan.

Task 3: Class Member Analysis & Recommendations

Assignment Questions and/or Required Screenshots Provided Below.

OBJECTIVE #1. Present your company disaster recovery and business continuity plan to a different class member and get a peer review.

Reviewer: Chris Lefebvre, March 17th, 2024

Disaster Recovery Section:

Step 5: You talk about creating a contact list for a group of employees/ external parties. Remember that the company should have people designated for the roles of the DRP, BCP.

A list of people involved in creating and working the DRP, BCP, IRP etc.

Stakeholders, Crisis management coordinators, Business continuity planning managers, recovery assessment technicians etc. Making the people and positions known is very important to people who want to know this information within your DRP. Just like you stated in your BCP on Step 4:

> **Step 5.** Next, we need to establish and create a contact list for the group of employees / external parties that will respond to disaster situations when they occur for the purpose of prioritizing communication and efficiency in DRP responses.

For Step 3 & 4, I would add a very small example of what YOU want for Microsoft. For example, set a certain goal you want to achieve for bring critical operations online (No more then 4 hours) “Time is money”. Same would go for your RTO.

> **Step 3.** Now that we have identified our main priorities of our disaster recovery plan, we then need to define a Recovery Point Objective (RPO), which is basically a threshold of what kind of data loss can be tolerated by the company and what kind of data loss poses a major risk to the company and must be recovered in the event of a disaster situation.

OBJECTIVE #2. Amend your plans to their suggestions.

Disaster Recovery Plan

The disaster Recovery Plan that I would implement for Microsoft would consist of the following steps:

Step 1. To properly follow the ERCM policy that governs disaster recovery plans, we would first need to conduct multiple test scenarios to determine the scale of potential threats to the company that the disaster recovery plan needs to address. This will help the Microsoft to determine which threats need to be more focused on than others due to the different levels of severity that each threat poses.

Step 2. After we identify the threats that Microsoft could potentially be faced with, we then need to analyze and identify what specific outcomes of the disaster recovery plan need to be prioritized. Given that Microsoft is one of the biggest technology companies in the world currently, I would imagine that they possess tons of crucial data that needs to be safeguarded at the highest level. I also would think that whereas Microsoft possesses data centers across the world that are critical to their daily operations, mitigating their system downtime in a disaster situation would be another top priority of the company.

Step 3 (Revised). Now that we have identified our main priorities of our disaster recovery plan, we then need to define a Recovery Point Objective (RPO), which is basically a threshold of what kind of data loss can be tolerated by the company and what kind of data loss poses a major risk to the company and must be recovered in the event of a disaster situation. I would believe that whereas Microsoft is a tech giant that has an extremely large number of consumers and businesses that rely on their services daily, the RPO would likely be centered around customer data, business data, financial data, and Employee data.

Step 4 (Revised). Now that we have defined an RPO to account for the threshold of what kind of data loss is and is not acceptable, we also need to create a Recovery Time Objective (RTO) to establish a threshold for how long their critical data center systems can suffer downtime before it begins to pose major risks to the company. While there are many factors that contribute to the specific target time an RTO should be set at, I would believe that the RTO should be set at no more than a window between 6-10 hours whereas Microsoft is a tech giant with an extremely large number of consumers / businesses that rely on their services.

Step 5 (Revised). Next, we need to establish and create a contact list for the group of employees / external parties that will respond to disaster situations when they occur for the purpose of prioritizing communication and efficiency in DRP responses. Some examples of the roles that staff members would be appointed could include Crisis Management

Coordinators, an Impact Assessment & Recovery Team, Business Continuity Experts, IT Application Monitors, and Executive Management.

Step 6. Now that we have laid the foundation for what problems we are addressing, what our priorities are, what our RPO/RTO is, and who will be responding to a disaster situation, we now must develop effective strategies to combat all types of disaster situations that may occur.

Step 7. Throughout the entirety of this process, we should be creating in-depth documentation of all aspects of the disaster recovery plan, as well as After action reports (per ERCM policy requirements) that outline the results of each review and must be reviewed by the ERCM team before it can be validated and established as an official backup plan.

Step 8. To align with the ERCM policy requirements, this disaster recovery plan will be extensively tested and reviewed at least every 12 months. Regularly reviewing the DRP documents will help to determine whether any changes or updates could be made to the DRP procedure to improve the effectiveness and efficiency of the DRP response operation, and it will enhance the efficiency of the operations by giving the response personnel practice in their roles in the event of a real DRP response.

Conclusion

In this document, I have successfully demonstrated the completion of the assignment requirements by conducting research on a company of my choosing and identifying factors that could influence their disaster recovery operations, identifying their regulatory bodies and compliance challenges that are associated, creating disaster recovery, backup, and business continuity plans for the company, and receiving feedback from a classmate regarding the plans that I created.

References

Acronis. (2023, September 28). *What is the difference between incremental, differential, and full backup?* Retrieved from Acronis: https://www.acronis.com/en-us/blog/posts/incremental-differential-backups/

Amazon. (n.d.). *What is Load Balancing?* Retrieved from Amazon: https://aws.amazon.com/what-is/load-balancing/#:~:text=Load%20balancing%20is%20the%20method,a%20fast%20and%20reliable%20manner

Aviture. (2023, April 12). *Data Encryption: Definition, Pros and Cons, and How It Affects You*. Retrieved from LinkedIn: https://www.linkedin.com/pulse/data-encryption-definition-pros-cons-how-affects-you-aviture/

BulletProof. (n.d.). *What Does the Consumer Privacy Protection Act Mean for Microsoft Customers?* Retrieved from BulletProof: https://content.bulletproofsi.com/what-does-the-canadian-consumer-privacy-protection-act-mean-for-microsoft-customers

Council of the European Union. (2018, May 25). *The general data protection regulation*. Retrieved from Council of the European Union: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/#:~:text=The%20European%20Data%20Protection%20Board,all%2027%20independent%20supervisory%20authorities.&text=Individuals%20can%20lodge%20a%20complaint,to%20judicial%20r

Dallabetta, P. (2022, February 22). *Data Replication Explained: Examples, Types, and Use Cases*. Retrieved from Redis: https://redis.com/blog/what-is-data-replication/

Flexential. (2023, August 17). *What is a disaster recovery team and who should be included?* Retrieved from Flexential: https://www.flexential.com/resources/blog/what-disaster-recovery-team-and-who-should-be-included

Government of Canada. (n.d.). *8 steps for planning your emergency and disaster plan*. Retrieved from BDC: https://www.bdc.ca/en/articles-tools/business-strategy-planning/manage-business/business-continuity-8-steps-building-plan

Heder, B. (2014, November 13). *Redundancy and failover and HA, oh my!* Retrieved from Network World: https://www.networkworld.com/article/932658/redundancy-and-failover-and-ha-oh-my.html#:~:text=Redundancy%20is%20having%20extra%20components,up%20a%20contingent%20operational%20plan

Hurley, J. (2021, August 5). *Failover, Redundancy, and Availability*. Retrieved from Smart File: https://www.smartfile.com/blog/failover-redundancy-and-availability

LinkedIn. (n.d.). *How can you measure backup performance?* Retrieved from LinkedIn: https://www.linkedin.com/advice/3/how-can-you-measure-backup-performance-m9oqf

LinkedIn. (n.d.). *What is the most effective way to measure your data storage and backup strategy?* Retrieved from LinkedIn: https://www.linkedin.com/advice/0/what-most-effective-way-measure-your-data-storage-d2moc#:~:text=You%20need%20to%20determine%20the,backups%20are%20complete%20and%20consistent

Maczka, P. (n.d.). *Pros and Cons of Cold Backup and Hot Backup. Comparison*. Retrieved from StorWare: https://storware.eu/blog/pros-and-cons-of-cold-backup-and-hot-backup-comparison/#:~:text=Availability%3A%20A%20cold%20backup%20requires,it%20remains%20available%20to%20users

ManageEngine. (n.d.). *What is data replication?* Retrieved from ManageEngine: https://www.manageengine.com/device-control/data-replication.html#:~:text=Data%20replication%20is%20the%20process,both%20individual%20computers%20and%20servers

Microsoft. (2023, June 5). *Resiliency and continuity overview*. Retrieved from Microsoft: https://learn.microsoft.com/en-us/compliance/assurance/assurance-resiliency-and-continuity#how-does-microsoft-test-business-continuity-and-disaster-recovery-plans

Microsoft. (n.d.). *Microsoft Data Centers*. Retrieved from Microsoft: https://datacenters-wp-production.azurewebsites.net/#:~:text=The%20Microsoft%20network%20connects%20more,global%20edge%20points%20of%20presence.

Miller, J. (2023, July 13). *The Importance of Encryption in Safeguarding Sensitive Data against Cyber Attacks*. Retrieved from LinkedIn: https://www.linkedin.com/pulse/importance-encryption-safeguarding-sensitive-data-against-miller/

Mohanakrishnan, R. (2021, November 23). *10 Best Practices for Disaster Recovery Planning (DRP)*. Retrieved from SpiceWorks: https://www.spiceworks.com/it-security/vulnerability-management/articles/best-practices-for-disaster-recovery-planning/

Patrizio, A., & Bigelow, S. J. (2023, October). *Microsoft*. Retrieved from Tech Target: https://www.techtarget.com/searchwindowsserver/definition/Microsoft

Quinn, A. (2023, November 20). *Business Continuity Roles and Responsibilities*. Retrieved from Continuity2: https://continuity2.com/blog/business-continuity-roles-and-responsibilities#:~:text=Direct%20Roles%20Within%20a%20Business,activities%20of%20business%20continuity%20management.

Stuflick, A. (2023, November 14). *Measuring Backup Performance - Essential KPIs to Track*. Retrieved from NovaBackup: https://www.novabackup.com/blog/measuring-backup-performance-essential-kpis

Tatum, M. (2024, February 25). *What is a Cold Backup?* Retrieved from EasyTechJunkie: https://www.easytechjunkie.com/what-is-a-cold-backup.htm

U.S. Department of Homeland Security. (2023, September 7). *IT Disaster Recovery Plan*. Retrieved from Ready: https://www.ready.gov/business/emergency-plans/recovery-plan#:~:text=Developing%20an%20IT%20Disaster%20Recovery,critical%20information%20is%20backed%20up

Vanover, R. (2024, February 5). *What is the 3-2-1 backup rule?* Retrieved from Veeam: https://www.veeam.com/blog/321-backup-rule.html