Ensuring Business Continuity: A Comprehensive Approach to Data Backup and Recovery

Slide 2

Good morning, everyone.

My name is Elliott and I am a student in the CTS 220 course double majoring in Cloud and Network Administration and IT Service and Support. My instructor for this class is Professor Green. Today, I am thrilled to share with you a project that I've been working diligently on for this honors presentation—My project scope focuses on ensuring the continuity of business operations through the development and implementation of an affordable and customized data backup plan for a local business here in Durham, named CSH Security. This presentation summarizes a 24 page backup and recovery plan for its design and implementation into the business.

In today's digital age, one fact rings true: Data reigns supreme. Whether you're a small family-owned business or a multinational corporation, the importance of safeguarding your data cannot be overstated. And that's precisely what brings me here today—to discuss how I've tackled this challenge for CSH Security.

Slide 3 - Overview of the Project

CSH Security, like many small businesses, relies heavily on its data for various aspects of its daily operations. These aspects include customer management, financial transactions, inventory tracking, and more. However, with the increasing volume of data comes the heightened risk of data loss or corruption. That's where my project comes in.

My objective was clear: to evaluate CSH's current data backup practices, identify any weaknesses or vulnerabilities, and develop a comprehensive backup plan tailored to their specific needs, user capabilities and accessibility, and budget constraints.

Slide 4 - Assessment of Current Data Backup Procedures

I began by analyzing CSH's existing data backup system and procedures. This included a combination of their on-premise server and a portable external USB drive. While CSH’s backup schedule was commendable, several weaknesses were identified, including non-structured backup policies and reliance on single-location storage. This reliance on a single point of failure could cripple the company should this data become lost, corrupted, or stolen. Even weather conditions here in North Carolina could cause data inaccessibility to this system thanks to a single point of failure.

Slide 5 - Regulatory and Industry Requirements

In building this backup plan, I ensured its compliance with industry standards and regulations, such as the General Data Protection Regulation (GDPR) and Health Insurance Probability and Accountability Act (HIPAA). These two regulations enforce strict requirements on all businesses that collect, process, and store personal and sensitive data from customers. I also followed guidelines from the National Institute of Standards and Technology (NIST) to help shape the plan itself. These standards cover topics such as data encryption, access controls, and regular checking and testing of in-use backup systems to ensure protection from and minimize the risk of data loss and theft.

Slide 6 - Designing and Implementing a Hybrid Data Backup Solution

To guarantee the resilience and future scalability of CSH's data backup strategy, I recommended that a hybrid solution utilizing the following technologies, which I will describe later, would benefit the company the best. A hybrid storage solution is one that has storage options both on premise and in the cloud. This hybrid approach follows the industry recommended 3-2-1 method of data backup and storage. The 3-2-1 method provides solid redundancy and flexibility features for the company's data accessibility. And now for a closer look at the Plan itself.

Slide 7 - Designing and Implementing 2

The 3-2-1 method is defined as having 3 backup copies (1 primary and 2 saved copies) on 2 different storage media types with at least 1 copy secure off site. This method ensures rapid and safe storage and recoverability from almost any disaster with the most minimal downtime incurred. For CSH's purposes, I also combined the grandfather – father – son (GFS) storage methodology into the 3-2-1 method. This storage scheme regulates the backup schedule criteria mandating the use of 3 different backup cycles. For this reason, I am using immediate use (Hot) storage, seldom use (Cold) storage, and rare / emergency use (Archive) storage options with each facet of the hybrid system backup plan.

Slide 8 - Selection of Backup Technologies, Services, and Solutions 1

First, let's discuss the hot storage component of the 3-2-1 method. CSH will continue using their portable hard drive for hot storage. This device facilitates the daily backup of critical files that are frequently accessed. This hot storage option ensures immediate access to essential data in case of emergencies. This device is kept on the owner's person for security reasons and data transportability.

Slide 9 – Selection of Backup 2

Next, for cold storage, a cloud service will be used in the backup strategy. Specifically, CSH will subscribe to the QuickBooks backup storage option, called Intuit's Data Protect Cloud Service. This option seamlessly backs up CSH's financial files to the cloud for off-premise storage. This subscription-based service offers automatic backups to a secure cloud storage, which guarantees the integrity and accessibility of their crucial financial data, regardless of on-site conditions. This solution provides an affordable peace of mind for the company.

Slide 10 – Selection of Backup 3

Given the current size of CSH Security, full-scale implementation of cloud storage isn't necessary just yet. Instead, for archive storage, data is backed up using a combination of the Windows backup and recovery program and a custom-built Network Access Storage (NAS) client using a reconditioned Dell desktop PC. The client's small special footprint and extreme storage capabilities make this a perfect fit for the company. I chose TrueNAS Core 13 for the NAS data storage management software. TrueNAS is the ideal choice for CSH as it is a free use service with an easy to navigate and command dashboard. The hard drive installed in the NAS client is a 10 TB hard drive specifically designed for NAS use. This is also perfect to handle CSH's current data volumes and offers plenty of growing room for the future.

Slide 11 – Selection of Backup 4

All archive backups, including a full system disk image (ISO) of the server, will be stored on their respective separate partitions on the NAS client hard drive. These backups occur every month using Windows Backup Scheduler and weekly using TrueNAS. This setup ensures redundancy and protection, with Windows backup handling the creation of the incremental backups and ISOs, while TrueNAS manages the creation of differential backups. By utilizing the secure connection and security features of OpenVPN, the TrueNAS archive drive client remains securely connected to the server network, even if stored off-premises. A VPN is a Virtual Private Network that creates a secure private connection between two devices over a public network.

As you can see, this hybrid system design not only safeguards the many cost-effective and sustainable recovery options, but also allows for future company scaling. By addressing fluctuations in access demand and availability, CSH Security can adapt to their evolving business needs seamlessly despite any potential disruptions.

Slide 12 - Price slide

I'd like to briefly highlight the estimated costs associated with implementing these new systems. The generalized total cost, including equipment, materials, time, and labor, comes to approximately $873.97 (taxes not included) for the primary components. With only a modest monthly service fee to Intuit QuickBooks for the Data Protect service, the ongoing expenses remain minimal. This ensures long-term affordability and efficiency with this backup plan.

Slide 13 - Documentation and Training

It is important for a proper backup systems maintenance regimen to have comprehensive documentation procedures and training programs that include proper backup procedures, backup policies, and disaster recovery plans. These are crucial to guide CSH and their employees through the backup and recovery processes. It is vital to regularly audit and update the documents to reflect any changes in backup systems, procedures, or business needs.

Slide 14 – Testing and Validation

This maintenance regimen also includes testing and validation of the backups and the systems at regular scheduled intervals using various methods. Some of which include checking the backups themselves, remaining disk storage capacity, disk health, network connectivity, that backup scheduling is active and properly configured, and the physical condition of the storage medias.

Slide 15 - Conclusion

In conclusion, my project highlights the critical importance of strong data backup and recovery strategies for businesses of all sizes. By implementing my comprehensive backup plan, CSH Security will be better equipped to minimize the risks of data loss and ensure the continuity of its operations.

Slide 16/17 - works cited

Slide 18 - Thank you for your attention and interest in my presentation. I'm happy to answer any questions you may have.