CTS 220
HONORS PROJECT 2024

Data backup and recovery plan for CSH Security

Abstract

This customized plan is tailored to CSH Security's smaller size, needs, and moderate budget. Work will begin by analyzing their current methods and setup to find the strengths and weaknesses of their system. Industry best practices will be used, ensuring compliance with all business, security, and safety regulations. The goal upon implementation, is to fortify CSH Security's data recovery abilities utilizing a custom designed data backup system and procedures.

Elliott Richter
[redacted]
Richterelliott3@gmail.com
CTS 220 Honors Project Spring 2024

Version History Log:

New Version #	Previous Version #	Revision Date	Author (full name, title, affiliation)	Location in Document and Description of Change	Reason for Change
1.0.0.0	0	05/03/24	Elliott Richter	Entire	Creation of Document

Contents

1. Introduction

In today's digital world, data ranks among one of the most valuable assets for a company, regardless of the company's size. Whether it's a home-ran business, a mom-and-pop storefront, growing chain franchise, or a multinational conglomerate, data can make or break the company. Small businesses, like CSH Security here in [redacted], rely heavily on their data files and customer information for numerous facets of daily operation. These include customer and order management, financial transactions, tracking inventory, logistics, and more. As the amount of this data increases, maintaining the complete integrity and security of such a vital part of the company becomes more difficult. The risk of data corruption or loss grows exponentially, especially if the company has a weak or even no data backup plan in place. Therefore, the integration of strong data backup procedures is paramount for ensuring the company's continued operation and to protect its confidential information.

This project evaluates the current data backup practices of CSH Security and creating and beginning implementation of a backup plan. As a small company, this plan is sufficient for their needs and a moderate budget. This project begins by analyzing their current methods and setup to find the strengths and weaknesses of their system. Industry best practices will be used, ensuring compliance with all business, security, and safety regulations. The goal is to fortify CSH Security's data recovery abilities.

The scope of this report includes an analysis of CSH Security's current data backup procedures, including a complete assessment of all hardware and software in use, the frequency of backups, any data retention policies, and security protocols for accessing and storing data. The objectives of this report cover identifying any weak points in the current procedures, re-aligning any practices that do not adhere to industry regulations and standards, and finally develop a comprehensive data backup plan specifically designed to fulfill the company's needs.

2. Assessment of Current Data Backup Procedures

CSH Security uses a combination of both an on-premise server and portable external USB hard drive for their data storage needs. The external hard drive is used specifically for data backup and file transportation. Incremental data backups, such as customer and order file management, are performed as needed after data is updated on the server. Full data backups, however, are usually performed every six months. These backups are stored with the daily backups on the external USB hard drive. Ideally, as the new backups are created, the older versions are deleted and replaced. This is done to preserve storage space on the hard drive.

Accessibility to the data and systems is decent with this setup, as all authorized users can access the server through a VPN (Virtual Private Network) connection or a remote desktop connection presuming they are authorized to do so. In addition, the external hard drive can be handed off to anyone who needs to use it, if they can physically be there to take possession of it.

After assessing CSH's data backup practices, several strengths and weaknesses have been identified. Their strengths include a backup schedule of around every six months of the financial, work, and customer files, with daily backups of the primary in use files such as the QuickBooks data. Data security on the server itself is strong as it is protected by a firewall and standard anti-malware software.

Their weaknesses, however, closely outnumber their strengths. This is understandable for a small company as the needs and infrastructures are vastly different than those of a larger company. Their weaknesses include their non-structured policies on backing up data, the procedures for physical and logical data security, and having all their data storage options in one location on-premises to name a few. In addition, utilizing only the built-in hard drives of the servers and the removable media for data backups and restoration are weak points in the security of the company's data. If either of these are damaged or stolen, both the primary and backup data files cannot be recovered. If there is any malware or data corruption on the primary files, it gets transferred to the same disks as the backups and the malware and / or corruption spreads. This also builds the potential for complete loss of data for the company.

CSH Security currently deploys an on-premise [redacted] edition for the Operating System. This particular server has a single Intel® Xenon® e-2314 CPU @ 2.8 GHz, 2808 Mhz with 4 cores and 4 logical processors. It also has 16 GB of ram installed. For storage they have 4 of 1 TB 2.5 inch 6k RPM SAS drives in a RAID 10 array for a total of 2.0 TB of useable storage not including the OS space requirements. For the portable backup storage CSH uses an external 2 TB USB hard drive. This is more than acceptable for the number and volume of files they save and transport on a daily basis. This server and company network is protected by a [redacted] firewall software. This firewall directly connects to the server, in addition to a company desktop and laptop. There is no switch on this network setup.

The person responsible for overseeing the data backup procedures is [redacted], the owner. She is solely responsible for managing the systems and procedures for data backup and restoration. As discussed in a later section, she will be trained to properly utilize and operate the backup systems and recovery protocols. Familiarity of these systems and their operation can only be strengthened by practice and time.

3. Regulatory and Industry Requirements

In addition to CSH's preferences and considerations to how their data is handled, the industry regulatory requirements and standards must also be adhered to pertaining to data protection and privacy. Of these regulations include the General Data Protection Regulation (GDPR) and the Health Insurance Probability and Accountability Act (HIPAA). These two enforce strict requirements on all businesses that collect, process, and store personal and sensitive data from customers.

Additionally, it is ideal to follow the industry best practices for data backup and recovery such as those set by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). 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.

Below you will find a summary of a few of the industry standards from and set by the NIST, condensed and summarized by ChatGPT with their correlating publication numbers that we will be adhering to:

"1. **Security Controls Selection (SP 800-53)**:

   - Provides guidelines for selecting security controls for information systems.
   - Includes recommendations for backup and storage controls to ensure data confidentiality, integrity, and availability.

2. **Contingency Planning (SP 800-34)**:
   - Focuses on developing comprehensive contingency plans for information systems.
   - Outlines procedures for implementing backup and storage strategies to mitigate risks and ensure continuity of operations.
3. **Protection of Controlled Unclassified Information (CUI) (SP 800-171)**:
   - Addresses requirements for protecting CUI in non-federal systems and organizations.
   - Includes provisions for data backup and storage to safeguard sensitive information from unauthorized access or disclosure.
4. **Storage Area Networks (SANs) Security (SP 800-125A)**:
   - Offers guidance on securing storage area networks (SANs) to protect stored data.
   - Includes recommendations for implementing backup and storage security measures within SAN environments.
5. **Cloud Computing Security (SP 800-162)**:
   - Provides an overview of secure cloud computing architecture.
   - Offers recommendations for data backup and storage in cloud environments, ensuring the security and integrity of stored data."

(Chat GPT, 2024) (NIST, n.d.)

4. Planning the Data Backup Strategy

The goals of CSH Security's data backup plan are to keep the security and accessibility of the critical business data intact, minimize any data loss or corruption from any cause, and be able to provide a rapid, efficient, and complete recovery in the event of a disaster. To do this, it is essential to identify the key goals in setting proper data backup priorities. These will be based on the data's importance, setting clear and concise procedures for [redacted] for the data backup and recovery processes, and aiding in the implementation of regularly scheduled backups and secure storage tailored to CSH's needs.

[redacted] and her associate will have the following responsibilities:

- Identifying and prioritizing critical data for backup within the company and ensuring the updated recommended procedures and policies are followed.
- Maintaining, managing, and monitoring the backup systems in addition to performing the scheduled backups and verifying their successful completion in full.
- Troubleshooting any issues which may occur and rectifying them.
- Ensuring the security and proper storage of the data backups by following industry guidelines.

Several backup and recovery options were discussed along with the company's capabilities and needs. Throughout the discussions the various plans were either redesigned or discarded until a consensus was achieved. Several cloud and on-premise system integration options were discussed. Although eh company has a modest budget to work with of $2,500, it was agreed that while it would be nice to have the fancy new systems, a simple redundant system is more than adequate and would save a large sum of money for company use.

For the targeted backup scheduling the following guidelines were created for CSH. The time between the backups and the schedule itself will be customized based on the frequency the data is accessed and updated in addition to its importance. Any critical data will have the highest priority, occur weekly or even daily if the information dictates. Other data, for example any monthly reports, correspondence, logs, any data deemed important, and system and server snapshots, will occur monthly. Overall server backups will occur every 6 months.

After reviewing and discussing what is deemed as critical data and superfluous data, the following actual data backup scheduling is being implemented. CSH Security will adopt the 3-2-1 rule for backing up their data using hybrid storage between on-premise and cloud storage. This involves having backups as 3 copies (1 primary and 2 saved copies), having these backups on 2 different storage medias, and finally having 1 copy offsite. This will ensure rapid and safe storage and recoverability from almost any disaster with the most minimal downtime. This method offers the best ease of use and accessibility experiences, while ensuring data integrity, security, and recoverability.

5. Selection of Backup Technologies, Services, and Solutions

Many current backup technologies are suitable for small businesses. These include cloud-based services, on-premises servers, and hybrid solutions. The decision in choosing which technologies to utilize was based on cost, scalability, reliability, and ease of implementation. A summary of the three categories of backup technologies we choose from are as follows:

- **Cloud-Based Backup Services**: Offer off-site storage, automatic backups, and scalability. Suitable for businesses with limited IT resources. Providers include AWS, Azure, and GCP.
- **On-Premises Backup Servers**: Provide control over data and may suit organizations with strict regulations or data sovereignty concerns. Options include dedicated appliances, software-defined storage, and tape systems.
- **Hybrid Solutions**: Combine cloud and on-premises infrastructure, offering cost-effectiveness and data protection. Enable local backups for quick recovery and off-site replication for disaster recovery.

It is agreed that a hybrid solution of available technologies would best suit CSH's current and future needs. And so, to accommodate the 3-2-1 method of data backup and storage, CSH Security will use the following devices and services in the recommended configuration and use for each system.

The data backup devices are intended to be complimentary to the internal hard drives located in the server. For the devices, CSH will continue using the portable hard drive for the hot storage. This includes the daily backing up of the critical files that will be accessed most frequently.

Next device is for the cold storage. Here a cloud service will be implemented. The QuickBooks backup storage option is a perfect fit for their financial files. This is a subscription service that automatically backs up the QuickBooks files to their server storage on the cloud. This will ensure that regardless of what disaster event occurs, no matter how big or small, the company's financial files will be easily recovered. These files are the most important to the owner and therefore will be kept securely off premise in the cloud. The backup storage service costs only $9.99 each month (QuickBooks, n.d.). This is extremely affordable for the company and is accessible anytime, anywhere.

Due to the current size of this company, CSH is not quite ready for Cloud storage. Until the company is ready to expand, for the archive storage, the data will be backed up using the Windows backup and recovery program and TrueNAS CORE software. The data, along with a system disk image (ISO) of the server, will be saved to a connected external hard drive, specifically the WD Red Plus 3.5" NAS HDD 10 TB, every month using Windows Backup scheduler and weekly using TrueNAS. I am using the WD RED 3.5" NAS HDD 4 TB as this drive is specifically designed for this application. 10 TB is a bit overkill for this company, but this size allows for long-term expansion and growth in addition to a larger backup history. The hard drive will have 3 partitions, one for the TrueNAS operating system, one for the Windows backup and restore, and once for the TrueNAS backup storage. The Windows backup will handle the incremental backups and ISOs, while the TrueNAS will handle the differential backups. This ensures that if one system is compromised, the other will be protected. The archive drive client (NAS PC) will be stored/located locked at a secure location chosen by the owner. If stored not on-premise, the archive drive will be connected to the server network over a VPN to aid in protecting the company data. For this service, we are using OpenVPN as it is secure and free.

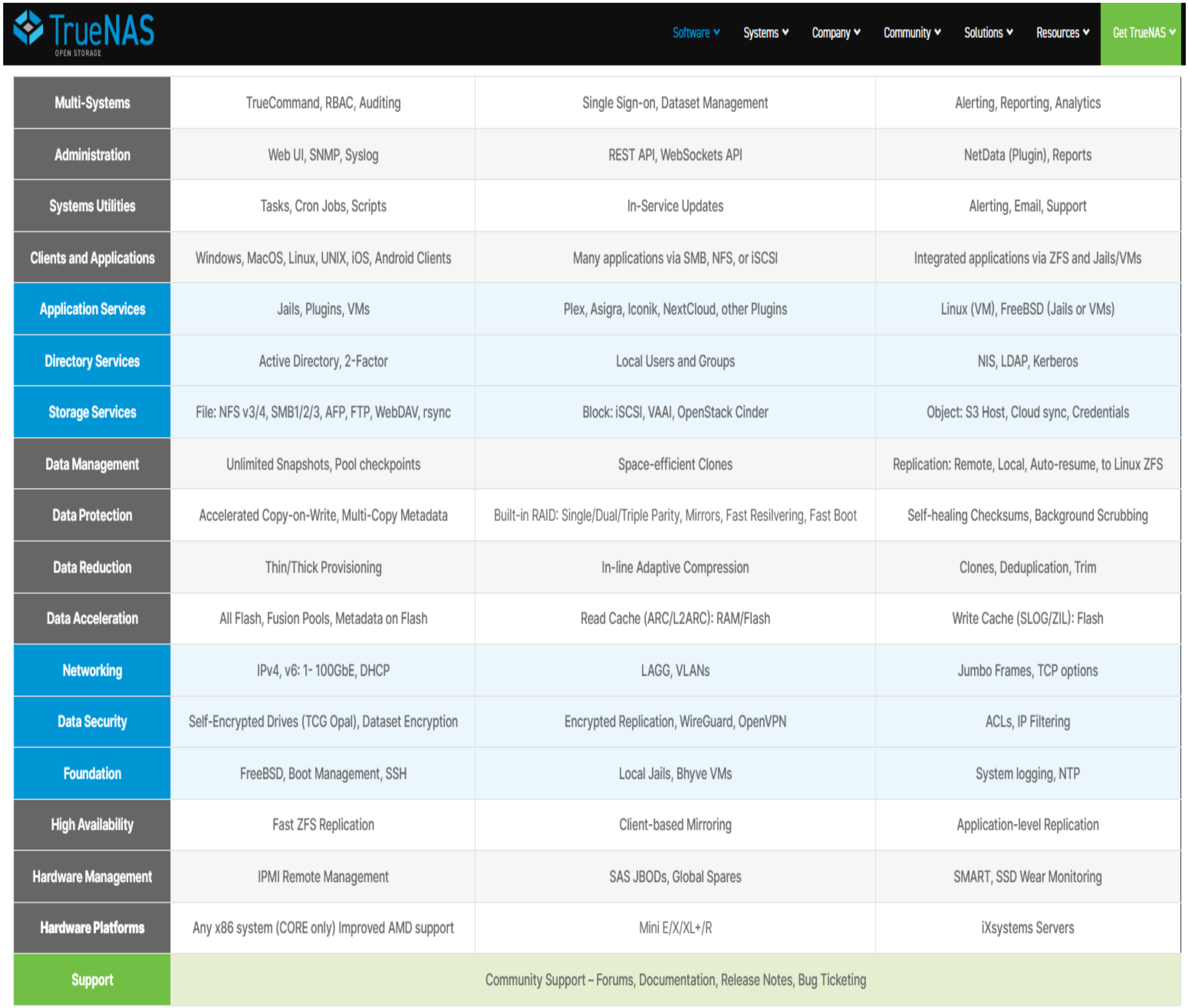
This system design for the 3-2-1 method allows for cost effective sustainability, while permitting future company scaling. The system will also allow for fluctuations in access demand and availability. Security is addressed in the system network firewall, authorized access, and VPNs. This will be addressed in more detail in the following sections.

A pricing table is included below to illustrate the general costs of installing the new systems. Equipment, materials, time, and labor are included and represent an estimate of the total cost minus taxes and any unforeseen expenses. The total cost for the additions and labor comes to approximately $873.97. This project price totals under budget for approximately $1,600. After this initial expense, the only reoccurring expense is the monthly service fee to Intuit QuickBooks for the Data Protect monthly service fee of $9.99.

Pricing Table:

Name	Quantity	Price	Total Price	Source	Use
Currently owned Equipment					
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Monthly Fees					
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
NAS System					
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Contractor Costs					
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			[redacted]		

Table of Features for TrueNAS CORE 13



Multi-Systems	TrueCommand, RBAC, Auditing	Single Sign-on, Dataset Management	Alerting, Reporting, Analytics
Administration	Web UI, SNMP, Syslog	REST API, WebSockets API	NetData (Plugin), Reports
Systems Utilities	Tasks, Cron Jobs, Scripts	In-Service Updates	Alerting, Email, Support
Clients and Applications	Windows, MacOS, Linux, UNIX, iOS, Android Clients	Many applications via SMB, NFS, or iSCSI	Integrated applications via ZFS and Jails/VMs
Application Services	Jails, Plugins, VMs	Plex, Asigra, Iconik, NextCloud, other Plugins	Linux (VM), FreeBSD (Jails or VMs)
Directory Services	Active Directory, 2-Factor	Local Users and Groups	NIS, LDAP, Kerberos
Storage Services	File: NFS v3/4, SMB1/2/3, AFP, FTP, WebDAV, rsync	Block: iSCSI, VAAI, OpenStack Cinder	Object: S3 Host, Cloud sync, Credentials
Data Management	Unlimited Snapshots, Pool checkpoints	Space-efficient Clones	Replication: Remote, Local, Auto-resume, to Linux ZFS
Data Protection	Accelerated Copy-on-Write, Multi-Copy Metadata	Built-in RAID: Single/Dual/Triple Parity, Mirrors, Fast Resilvering, Fast Boot	Self-healing Checksums, Background Scrubbing
Data Reduction	Thin/Thick Provisioning	In-line Adaptive Compression	Clones, Deduplication, Trim
Data Acceleration	All Flash, Fusion Pools, Metadata on Flash	Read Cache (ARC/L2ARC): RAM/Flash	Write Cache (SLOG/ZIL): Flash
Networking	IPv4, v6: 1- 100GbE, DHCP	LAGG, VLANs	Jumbo Frames, TCP options
Data Security	Self-Encrypted Drives (TCG Opal), Dataset Encryption	Encrypted Replication, WireGuard, OpenVPN	ACLs, IP Filtering
Foundation	FreeBSD, Boot Management, SSH	Local Jails, Bhyve VMs	System logging, NTP
High Availability	Fast ZFS Replication	Client-based Mirroring	Application-level Replication
Hardware Management	IPMI Remote Management	SAS JBODs, Global Spares	SMART, SSD Wear Monitoring
Hardware Platforms	Any x86 system (CORE only) Improved AMD support	Mini E/X/XL+/R	iXsystems Servers
Support	Community Support – Forums, Documentation, Release Notes, Bug Ticketing		

(TrueNAS, n.d.)

6. Procedures for Testing and Validation

Procedures for testing and validating backups have been developed for CSH to ensure functionality, data integrity, and recoverability. Backup tests will be conducted regularly, following the predefined recommended methods and schedules. Testing frequency will vary based on the importance of the data and the system used for the backup environment.

Backup tests for each system include:

- Verifying the system's operation.
- Verifying the system's security by checking logs.
- Verifying the integrity of backup files.
- Simulating data restoration processes to ensure effective and timely recovery.
- Testing disaster recovery plans to validate their effectiveness in real-world scenarios.
- Conducting periodic audits to assess compliance with backup procedures and industry standards.
- Audits will be inspected to identify areas for improvement.

The testing and validation procedures for the hot storage, external USB hard drive, include inspecting the disk health, operation, storage used, and accessibility. Once connected, the drive will be inspected using Device manager. Disk properties will display the condition of the drive's usage and allow for a health check to be performed. This will identify and repair any bad sectors that may exist. File integrity will be checked by simply copying and pasting files to the drive and testing if they open successfully with all data intact.

Testing and validation procedures for the cold storage system, Intuit Quickbooks Data Protect, is as simple as logging into QuickBooks online and checking the status of your account. Here the data and settings can be checked for the proper configurations and timestamps. In addition, the subscription status and billing will be checked for accuracy and active status. If any discrepancies exist in any of the aforementioned areas, immediate correction will begin. Next, test the recoverability of the data by following the service prompts to download the data and attempt opening the file on the local computer using the QuickBooks software.

For the archive storage, the TrueNAS system, majority of the testing and validation procedures can be done from anywhere CSH's network is accessed. The TrueNAS system dashboard is accessed via internet browser and any configuration and status updates can be found here. This includes event logs for the system, which will be checked weekly. On this dashboard, system status, storage usage, configurations, and more are displayed. Alerts can be set up for any system anomalies that may occur. Data can be accessed through this dashboard and recovered onto the server for integrity testing. Off-premise validation of the NAS system itself includes network accessibility and operation. If there is a problem with either of these, direct hands-on inspection is required.

The physical validation processes for the TrueNAS are the only process that must be completed on-premise at the location where the NAS is stored. If it is the same location as the server, then all connections can be inspected at the same time. If stored separate from the server, connections and inspection must be completed at both locations. For inspecting the NAS, a visual inspection includes checking all connected wires and status lights indicating operation. Look for any damage to the wires or system itself or its environment. If any issues are found, fix immediately and check connection to the system via the dashboard.

7. Contingency Planning

Contingency plans have been developed to address any potential failures or disruptions in the backup process. The contingency plans outline alternative backup solutions and recovery strategies to minimize downtime and data loss in the event of a backup failure or disaster. For the scope of this project, any non-IT related, personnel, HR, or property related disasters are not considered in this disaster recovery plan overview. A complete and more comprehensive plan will be designed and created for CSH upon request but will constitute as a separate service, scope, and will be billed accordingly.

CSH's Contingency planning covers:

- Identifying backup alternatives, such as redundant backup systems, cloud-based backups, or manual backup processes.
- Frequent regular testing and monitoring of CSH's systems.
- Utilizing Incremental and Differential backups.
- Establishing recovery procedures for restoring data from backups in the event of a failure.
- When to implement said recovery procedures and persons authorized to do so.
- Documenting escalation procedures for notifying responsible parties to aid in the recovery process and initiating recovery actions.
- Conducting regular reviews and updates of contingency plans to ensure their effectiveness and relevance to modern day technologies and scenarios.

Several contingency plans have been developed for CSH in the event of a disaster scenario. Some examples of what constitutes a disaster scenario include events that fall under natural disasters (hurricanes, floods, etc.), external/infrastructure disasters (power outages, construction, etc.), cyberattacks (ransomware, viruses, etc.), physical attacks/theft (robbery, vandalism, human error, etc.), regulatory compliance issues (non-compliance with sensitive data that can lead to legal issues or data loss), and/or Force Majure events (sudden equipment failure, bad sectors, etc.). By implementing these contingency plans and recovery strategies, CSH Security aims to mitigate the risk of data loss and ensure the continuity of operations, even in challenging circumstances.

The phases of these Disaster Recovery Plans (DRP) include the activation and notification phase, recovery phase, and reconstitution phase.

According to the University of Southern California, the phases can be summarized as:

> “
>
> 1. Activation and Notification Phase – Activation of the IT DRP occurs after a disruption or outage that may reasonably extend beyond the recovery time objective (RTO) established for a system.

> Once the IT DRP is activated, system owners and users are notified of an outage and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.
>
> 2. Recovery Phase – The recovery phase provides formal recovery operations that begin after the IT DRP has been activated, outage assessments have been completed, personnel have been notified, and appropriate teams have been mobilized. Recovery phase activities focus on implementing recovery strategies to restore system capabilities through the restoration of IT components, repair of damage, and resumption of operational capabilities at the original or new permanent location. At the completion of the recovery phase, critical services will be functional and capable of performing the intended functions.
>
> 3. Reconstitution Phase – The reconstitution phase defines the actions taken to reconstitute systems in the original data center or in extreme cases, in the new permanent data center. This phase consists of two major activities: validation of successful recovery and deactivation of the plan. During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing. Deactivation includes activities to notify users of the system's normal operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future recovery events.
>
> " (USC, n.d.)

Upon a disaster occurring [redacted] will be notified along with anyone she hires to manage her network and data systems. Once the systems are back to normal secure operations, the data will be recovered using one of the three backup systems, depending on the severity of the data loss. For most disaster recoveries, restoring the data from the external USB drive will be sufficient. For more severe data loss events, restoration from the NAS will be the next level of escalation.

Should the disaster be due to cyberattacks, a thorough inspection of the data backups will need to be performed. Isolating when the malicious software was installed or when the attack occurred is crucial in selecting the proper backup to restore. This is where the incremental backups and differential backups come into play. Typically, the differential backups will be of no use in these situations as the malware or corrupted data has a high probability of being on the backup. By isolating the date of the attack or corruption, a backup from an earlier time can be chosen to restore the data with as minimal loss as possible. Anything sooner will simply reintroduce the corrupted data or malware back into the system. Since the financial files are the most crucial data for the company, the QuickBooks Data Protect subscription offers the most secure and reliable backup option for this type of data. However, keep in mind this does not protect any other data on the system.

After the data is recovered, verification will commence. This is where [redacted] will inspect the integrity of the data and verify that the information is intact. This can be done by comparing it to other backups if applicable. Next it is important to document the disaster event and the recovery processes for reference and auditing. More on the documentation and training in the next section.

8. Documentation and Training Procedures

Comprehensive documentation procedures and training programs that include proper backup procedures, backup policies, and disaster recovery plans are crucial to guide [redacted] and her 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.

Various templates and forms are available online and [redacted] will be able to choose the one that best fits her company's needs and style of operation. For the documentation procedures, storing the documents, and management of said documents, we will briefly cover a few topics below.

Documentation must be kept showing the devices and software used in the data backup process. In addition, all personnel who have access to and manage these backups will also need to be recorded. It is best practice to log the dates, times, and systems for when the backups take place. Any errors, issues, or disasters will be recorded in the log as well. Ownership/possession of any removable devices, namely the external USB drive, will also be logged when possession is transferred to another individual. Other important information to log is emergency contacts, account information, and support numbers for all equipment and services CSH owns or subscribes to. This should be managed by [redacted] and any personnel she deems trustworthy. A comprehensive list of equipment inventory assets should be maintained for recovery and insurance purposes.

The blank forms for documentation should be readily accessible, while the filled out should be stored in secured locations that are a part of the data backup operations. Additionally, all training documentation and programs should be backed up and accessible as well. All above mentioned documents are set to be backed up on the TrueNAS and external USB drive.

Training sessions on the operation of each backup and recovery system will be offered to [redacted] to guarantee a solid understanding of backup procedures. This training covers the following:

- Best practices and regulations for the backup and data recovery methods.
- [redacted] and any other personnel's role and responsibilities in the backup and recovery processes.
- The specific operation of all backup systems and their configurations.
- Understanding and operation of the TrueNAS dashboard and network connection.
- How the data backups are stored both on-premise and in the cloud.
- Proper scheduling and location of Windows Backup and Restore with ISO backups.
- Data restoration and documentation processes for data recovery.
- How to test and validate the data backups and recovery.
- Choosing an effective contingency plan and DRP templates.

- How to document, store, update, and audit the documentation and procedures.
- Verifying security protocols on all data backup storage devices and locations.

9. Presentation and Implementation of the Backup Plan

CSH is presented with this project report for review, approval, and implementation. This project will also be presented at [redacted] Community College's Honors class symposium on [redacted]. All confidential information will be redacted for this college presentation prior to the presentation date. CSH's and the symposium presentations will include an executive summary of all important findings, recommendations, and all implementation steps for this backup plan. CSH will also be presented with a letter of intent, budget pricing chart, and other relevant documentation for the implementation of the plan. [redacted] feedback will be requested and integrated into the final backup plan before implementation begins. Implementation will begin after final approval of the backup plan at Miss Butler's discretion.

10. Conclusion

In conclusion, it is essential for CSH Security to implement into their operations this comprehensive data backup and recovery plan. This plan will be the first step in ensuring the integrity, availability, and security of the company's critical data. This plan is designed to be easily integrated, understood, and followed while being affordable and fulfilling CSH's business needs. Throughout the creation of this plan, CSH's current infrastructure and procedures, planning backup strategies, integrating the appropriate backup technologies, and implementation of procedures for testing, validation, guidelines for contingency planning, documentation, and training have been assessed and custom tailored to CSH's specific business needs. It is recommended to implement a DRP and documentation system that best fits into the company's current operations. CSH Security can better mitigate the risk of data loss and ensure business continuation despite potential disruptions or disasters.

Letter of Intent

Elliott Richter
[redacted]
Richterelliott3@gmail.com
[redacted]

[redacted]
CSH Security Systems, Inc.
[redacted]

Dear [redacted],

I am writing to express my intention to work with CSH Security on a project aimed at upgrading the data backup and protection policies for your company. As a student undertaking an honors project, I am eager to offer my knowledge and skills to support CSH Security in implementing a comprehensive data backup plan tailored to your specific needs.

The purpose of this project is to evaluate your current data backup practices, identify the areas that can be improved upon, and offer my recommendations for improving and assistance in implementing the proposed plan for your data backup and protection policies and systems. Industry best practices will be used, ensuring compliance with all business, security, and safety regulations while we fortify CSH Security's data recovery abilities. I will provide awareness to areas that can benefit from improvement and develop a reliable plan for strengthening data storage and security while minimizing the risk of data loss or corruption.

The scope of the project will include:

- Evaluating the status of your current data backup systems and policies.
- Industry best practices will be used, ensuring compliance with all business, security, and safety regulations.
- Developing a thorough data backup plan aligned with CSH Security's security and storage requirements.
- Providing my recommendations for selecting the best fit backup options and cloud services, setting backup schedules, and implementing the agreed upon plan while testing the new company procedures and systems.
- I will offer guidance on contingency planning, proper documentation, employee training on the implemented system, and company communications.

I am excited and dedicated to working closely with CSH Security throughout this project to make sure that this proposed data backup plan aligns with your organization's goals and priorities. Working together and clear communication will be essential aspects in the success of this project, and I am dedicated to maintaining open communication and addressing any questions or concerns that may arise.

I am excited about this opportunity to help in advancing the success of CSH Security and I am confident that together, we can enhance your data backup and protection policies to ensure the security of your critical business assets, thus ensuring your company can continue its daily operations regardless of any potential disruptions you may incur.

Thank you for considering my project proposal. I am excited to work on this project with you and help your company be more secure in its data backup procedures. I am available at your convenience to schedule a meeting or provide additional information to answer any questions or concerns you may have.

Sincerely,

Elliott Richter

Network and Cloud Administration / Virtualization

and IT Service & Support Student

Works Cited

Bigelow, S. J. (n.d.). *The 7 critical backup strategy best practices to keep data safe*. Retrieved from TechTarget: https://www.techtarget.com/searchdatabackup/feature/The-7-critical-backup-strategy-best-practices-to-keep-data-safe

Chat GPT, E. R. (2024, March 24). *Chat GPT*. Retrieved from Chat GPT: https://chat.openai.com/

Cohesity. (n.d.). *Cohesity Cloud data management*. Retrieved from Cohesity: https://www.cohesity.com/products/data-cloud/

Druva. (n.d.). *Druva website*. Retrieved from Druva: https://www.druva.com/products/pricing-plans

Heckathorn, P. R. (n.d.). *Data Backup Options*. Retrieved from cisa.gov: https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf

ITGlue. (2022, March 9). *SOP Documentation: A Guide for Writing Standard Operating Procedures*. Retrieved from IT Glue: https://www.itglue.com/blog/sop-documentation/

Jerry. (15, March 2024). *How to create an ISO Image from your operating system*. Retrieved from EaseUS: https://www.easeus.com/backup-utility/create-an-iso-image-from-your-operating-system.html

LinkedIn. (n.d.). *How can you ensure your backup and recovery processes meet industry standards?* Retrieved from LinkedIn: https://www.linkedin.com/advice/0/how-can-you-ensure-your-backup-recovery-hg2be

LinkedIn. (n.d.). *What are the best data storage and backup options for small businesses?* Retrieved from LinkedIn: https://www.linkedin.com/advice/0/what-best-data-storage-backup-options-small-businesses

Microsoft. (2024, April 7). *Azure Blob Storage Pricing*. Retrieved from https://azure.microsoft.com/en-us/pricing/details/storage/blobs/

NIST. (n.d.). *Protecting Data From Ransomware And Other Data Loss Events*. Retrieved from National Cybersecurity Center of Excellence: https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf

QuickBooks, I. (n.d.). *Intuit Data Protect*. Retrieved from Intuit QuickBooks: https://quickbooks.intuit.com/intuit-data-protect/

Rubrik. (n.d.). *Cloud data management*. Retrieved from Rubrik: https://www.rubrik.com/solutions/cloud-solutions

TrueNAS. (n.d.). *TrueNAS CORE*. Retrieved from TrueNAS: https://www.truenas.com/truenas-core/

USC, U. o. (n.d.). *University of Southern California IT Disaster Recovery Plan Template*. Retrieved from USC.edu: https://customsitesmedia.usc.edu/wp-content/uploads/sites/532/2019/02/21035639/Disaster-Recovery-Plan-Template.pdf