**Lack of Redundant Networks and Why it is Important in Business:**

**A Case Study.**

Michael Winder

University of Wisconsin – Stout

ICT 701: Information and Communication Technologies in Organizations

Dr. Laura Reisinger

February 28, 2024

Table of Contents

[Introduction 2](#_Toc159256430)

[Background 3](#_Toc159256431)

[Proposed Technology Solution 4](#_Toc159256432)

[Impact Analysis 6](#_Toc159256433)

[Recommendation 7](#_Toc159256434)

**Introduction**

As most people know, within the landscape of modern business, adapting to changing circumstances often involves restructuring and redefining the foundational aspects of day-to-day operations. Such is the case for my current organization, which recently underwent a separation from its original company. While most of the time this would not be anything to cause concern, this separation led to the company establishing an independent network infrastructure. In the process of this separation, a critical vulnerability arose – the absence of a redundant network. This absence exposes the company to the immediate risk of a single point of failure should a network outage occur, a situation that has been acknowledged as a priority that needs to be addressed by information technology staff and management.

 In response to this need, we are embarking on a strategic initiative to create a secondary data center. This secondary data center is envisioned not only as a repository for additional physical servers and databases, but also as a location for redundant internet connections. The objective is clear – to fortify the company’s network infrastructure and ensure continuity of operations in the face of unforeseen challenges. However, the realization of this critical undertaking is contingent upon several factors. It is subject to the constraints of the IT budget allocated for new equipment in this fiscal year. Additionally, approval for an increase in monthly expenses for the internet connections is a pivotal consideration. In recognizing this importance, the company has opted to leverage internal resources for this project, thereby minimizing costs associated with external Managed Service Providers (MSP).

 The timeline for this initiative is set to be completed by the middle of fiscal year 2025. This period allows for meticulous planning, thorough testing, and collaboration with Internet Service Providers (ISPs) to establish new circuits to the locations requiring connectivity. As we move forward on the journey, the focus will remain on fortifying the network infrastructure, ensuring the resilience and reliability that is necessary for the seamless provision of our healthcare services.

**Background**

 The issue in question, a lack of a redundant network for the company started just this past October when the company began the complete separation from the original parent company. With two different divisions this was a multi-tiered separation. First, we transitioned the three locations that cover one aspect of the company, this was a single weekend project, followed by a week of troubleshooting issues. The following weekend, we completed the separation by moving the remaining ten locations over to the new network. This again was followed by a week of troubleshooting. This is when the major issue began. After the migration of end user devices to the new network, the configuration was a hub-and-spoke topology, with the primary internet feed residing in a data center that we co-locate within.

This centralized data center leaves the company vulnerable to disruptions should there be an internet outage, potentially hindering the ability to access vital information and applications that are hosted on cloud services. Which in turn can lead to a delay in patient care, along with possible reputational damage based on this delay. Given the nature of the healthcare business, where uninterrupted access to the internet and network communications are imperative for patient care, along with treatment reviews, the creation of a redundant system becomes paramount.

Socially, the creation of a redundant network aligns with the importance of uninterrupted network communication for healthcare professionals to deliver quality patient care and treatment reviews. From a technological standpoint, the project necessitates adopting a solution to establish a robust secondary data center along with a secondary Internet Service Provider (ISP). This is important based on an article by Kevin Dooley where he states, “it is crucial to have redundant networks with flexible internet access. Businesses cannot operate if the network is down—continuous internet connections and functioning technology are essential these days.” (Dooley, 2023). Economic considerations come into play, with the budget influencing the scale and capabilities of the project, along with its increased internet costs that could influence decisions. Environmentally, the project must adhere to company and regulatory practices to ensure the new data center's efficiency. Politically, the project may hinge on government regulations and policies affecting data centers, internet infrastructure, and healthcare IT. Legally, compliance with data center regulations, particularly as stated within HIPAA, is imperative. Ethical considerations look at the responsibility of a company to transparently manage patient data. This is made apparent in the security rule portion of the HIPAA Act, where it states that “The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI) (hhs.gov, 2022).

**Proposed Technology Solution**

In the realm of enterprise networking, the choice of network devices plays a pivotal role in shaping the efficiency, reliability, and security of an organization's digital infrastructure. This is especially true when working to add redundancy to the network. This analysis will look at three different manufacturers of network devices offered by leaders within the industry. We will also analyze which one may be a better solution for within the company. The table below shows a comparison of the three chosen manufacturers and the products that are being considered for this project.



Table 1: Pricing from CDW.com at <https://www.cdw.com>

HP Devices

The HP HPE-1950-48G-2SFP+-2xgt-POE is a robust networking switch featuring 48 ports, two SFP+ ports, and two Gigabit ports with Power over Ethernet (PoE) capability. Its manageable nature makes it suitable for enterprises seeking control over their network infrastructure. With a moderate cost of $1,314.93 per unit and a requirement of two units, it offers an attractive balance of features and affordability. The HPE Aruba FlexNetwork MSR3016 is a versatile multi-service router designed to meet the complex networking needs of enterprises. It offers manageability and a plethora of ports to facilitate seamless connectivity. However, its higher cost of $3,227.99 per unit might be a deterrent for organizations with budget constraints.

Cisco Meraki Devices

The Cisco Meraki MS410-16 switch is a compact yet powerful solution, featuring 16 manageable ports. Priced at $8,073.99 per unit and requiring two units, it falls on the higher end of the cost spectrum. Nevertheless, its advanced management capabilities and robust performance make it a compelling choice for large-scale deployments. The Cisco Meraki MX85 is a security appliance equipped with eight manageable ports, offering comprehensive network protection and management functionalities. With a price tag of $2,115.99 per unit, it presents an attractive option for organizations prioritizing security without compromising on cost-effectiveness.

Cisco Devices

The Cisco ISR4431 router boasts four manageable ports and advanced features suitable for enterprise networking environments. Priced at $6,419.99 per unit, it represents a considerable investment, albeit justified by its robust performance and scalability. The Cisco Catalyst 9300 switch is a highly configurable device featuring 24 manageable ports, catering to the diverse needs of modern enterprises. With a cost of $5,374.99 per unit and a requirement of two units, it strikes a balance between performance, scalability, and affordability.

**Impact Analysis**

 While the different proposed solutions will not be initially implemented at all locations, as it primary issue is no redundancy with the overall connection to the internet. This solution will be implemented within the main datacenter location as a backup to the primary internet connection for the company. Not only will there be the cost of the new equipment, but we must consider the time for installation and the costs of a secondary Internet Service Provider (ISP) to install and maintain a connection to this location.

Some immediate impacts to the organization would be initial costs of equipment and an increase in costs for internet. On the other hand, the return on investment (ROI) would be that downtime and loss of patient care would be minimized and become almost non-existent. If we were to look at some analysis of the overall impact of the proposed changes, we could see that socially this would show the company focusing on increasing reliance on digital connectivity along with a growing emphasis on network security. These changes would also allow the company to delve into technology that is considered modern or innovative by allowing the use of Software Defined Networking (SDN) and even looking at things like Artificial Intelligence (AI) or Machine Learning (ML) to assist in switching between ISPs should be need arise. While economically, as mentioned above, upfront costs would be higher, the overall ROI would offset these costs over a two-year period based on the calculations mentioned in a report by the KR Group that states, “Calculating the cost of user downtime is relatively straightforward. You take the hourly payroll rate for affected employees and multiply it by the length of the outage” (Keeler, 2021). While many companies are concerned about the environment this day in age, the minimal amount of electricity that would be used to add to this redundancy is of minor importance overall. All the devices that are being looked at also comply with all needed federal regulations that the company must abide by at this time. This includes things like data governance, cybersecurity practices, and HIPAA regulations.

**Recommendation**

After carefully considering all the options available, leveraging the Cisco ISR4431 and Catalyst 9300 devices for network infrastructure represents the best strategic investment for the organization to increase the company’s resiliency. By prioritizing reliability, scalability, and redundancy, the Cisco solution can mitigate operational risks, ensure business continuity, and empower the organization to achieve their objectives with confidence. As such, the decision to embrace Cisco products transcends mere cost considerations, embodying a strategic commitment to excellence and innovation in network infrastructure.

While these Cisco products may come with a higher upfront investment for the organization, an upfront cost of $18,000, it is essential to evaluate the comprehensive value they provide. The Cisco ISR4431 router offers advanced features and scalability, ensuring efficient network operations and can help with accommodating future growth. Similarly, the Catalyst 9300 switch delivers high performance, reliability, and flexibility, supporting diverse networking requirements with ease. Moreover, Cisco's reputation for quality and reliability typically instills confidence in all IT decision-makers, mitigating concerns about operational risks and downtime. The long-term benefits of Cisco's industry-leading solutions, including enhanced productivity, reduced maintenance overheads, and seamless scalability, outweigh the initial cost differential.

Implementing a redundant network solution with Cisco devices is essential for mitigating risks associated with network downtime. This solution will also easily integrate with the existing solution of Meraki as they are from the same manufacturer. The ISR4431 router and Catalyst 9300 switch provide robust failover capabilities, ensuring uninterrupted connectivity even in the event of hardware failures or network disruptions. By deploying redundant components strategically, this organization can minimize the impact of potential outages on critical operations, maintaining business continuity and preserving service levels. This initiative-taking approach not only enhances reliability but also reinforces organizational resilience, bolstering confidence among stakeholders and safeguarding against unforeseen challenges.

Failure to implement a redundant network solution could potentially expose the organization to various risks, including productivity losses, revenue decline, and reputational damage. Without failover mechanisms in place, even a minor network disruption could disrupt operations and compromise customer satisfaction.

By leveraging Cisco ISR4431 and Catalyst 9300 devices for network infrastructure, organizations can effectively address this issue. These devices offer built-in redundancy features, such as Hot Standby Router Protocol (HSRP), enabling seamless failover and ensuring uninterrupted connectivity. This is corroborated by WireX, “HSRP ensures continuous network connectivity by electing active and standby routers based on priority values and utilizing a virtual IP and MAC address that are shared among group members. This process allows for a seamless transition when a router fails, thereby minimizing disruptions to the network” (wirexsystems.com, 2023). As a result, organizations can maintain business continuity, uphold service levels, and mitigate the impact of network disruptions on their operations.

References

(OCR), O. for C. R. (2022, October 20). *Summary of the HIPAA security rule*. HHS.gov. <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>

*CISCO 4000 Series Integrated Services Routers*. Cisco. (2024, February 23). <https://www.cisco.com/c/en/us/products/routers/4000-series-integrated-services-routers-isr/index.html>

*Cisco Catalyst 9300 Series Switches Data Sheet*. Cisco. (2024b, April 12). <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html>

Dooley, K. (2023, August 29). *Network redundancy and why it matters*. Auvik. <https://www.auvik.com/franklyit/blog/simple-network-redundancy/>

HIPAA-compliant data centers. (n.d.). <https://www.hipaajournal.com/hipaa-compliant-data-centers/>

*HPE networking comware router AC MSR3016*. HPE Store Singapore. (n.d.). <https://buy.hpe.com/sg/en/networking/routers/modular-ethernet-routers/msr-modular-products/hpe-networking-comware-router-ac-msr3016/p/r8v32a>

HPE OfficeConnect 1950 switch series. (n.d.). <https://www.hpe.com/psnow/doc/c04545486.pdf?jumpid=in_pdp-psnow-qs>

Keeler, M. (2021, September 10). *The roi of a well-planned network: KR Group*. The KR Group, Inc. <https://www.krgroup.com/roi-well-planned-network/>

*MS410-16*. Cisco Meraki. (2023, September 28). <https://meraki.cisco.com/product/switches/aggregation-switches/ms410-16/>

*MX85 datasheet*. Cisco Meraki Documentation. (2024, April 4). <https://documentation.meraki.com/MX/MX_Overviews_and_Specifications/MX85_Datasheet>

Preusz, B. (2023, August 9). *HIPAA compliance for IT professionals in 2023*. Les Olson IT. <https://lesolson.com/blog/hipaa-compliance-for-it-professionals/>

*What is HSRP? understanding network protocols by WIREX Systems*. WireX. (2023, April 23). <https://wirexsystems.com/resource/protocols/hsrp#:~:text=HSRP%20ensures%20continuous%20network%20connectivity,minimizing%20disruptions%20to%20the%20network>