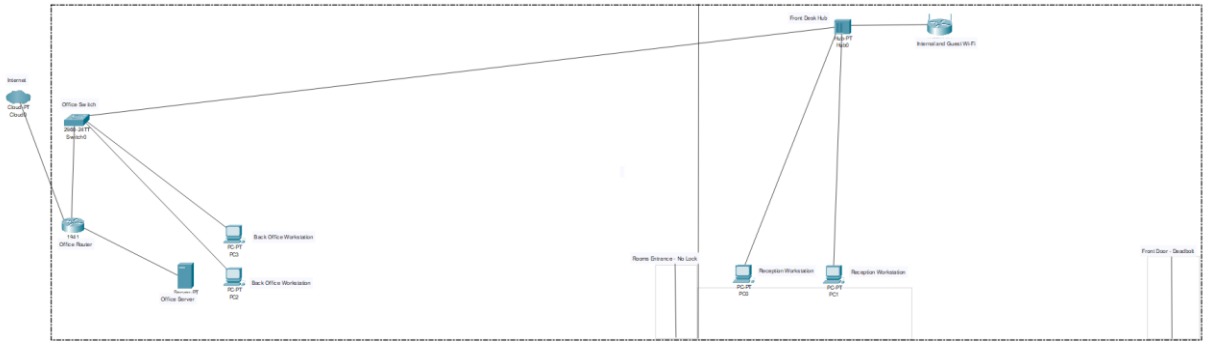
Andree Salvo

Southern New Hampshire University

CYB 420

Instructor: William Mitchell

1-2 Project One Stepping Stone: Risk Domain Analysis



Vulnerability One

Risk Domains:	From the given scenario, this falls under the technological risk domain because it involves issues with network performance, data loss, and communication disruptions.
Security Controls:	• **Conduct data integrity verification:** Implement hashing methods to safeguard data during storage and transfer, helping detect tampering or corruption early. • **Implement network segmentation:** Network segmentation is needed to improve performance and security by isolating critical systems and controlling traffic flow. This helps prevent network delays and limits unauthorized access or threats from spreading. • **Quality of Service (QoS):** Applying QoS will help manage network traffic

	to ensure that important data gets the priority it needs. • **Utilizing Data backups**: If your data is not recoverable from network issues, back up your data immediately to a safe location or cloud.
Mitigating Risk:	These controls protect healthcare records from tampering, ensure accurate data access, and prevent system disruptions, improving reliability and reducing downtime.

Vulnerability Two

Risk Domains:	This falls under **people and processes** because it involves how employees manage access to restricted areas and how the organization establishes procedures to protect sensitive physical assets, such as medicine and patient records, in compliance with HIPAA requirements.
Security Controls:	• Implement Role-based access controls (RBAC) because we need to give employees the right permissions for their specific roles. • Implement restricted keycards • Creating a stronger policy and process for HIPAA compliance when handling or managing patient data, storage, and assets to educate employees on HIPAA regulations.
Mitigating Risk:	Implementing these controls will help safeguard patient data, assets, and medicine. etc., ensuring everyone adheres to HIPAA compliance and limits physical access to restricted areas, products, and patient data.

Vulnerability Three

Risk Domains:	This is a **technology** risk domain as it involves securing remote connections for employees to access their data on an offline server
Security Controls:	**Security controls I would implement are:**

	• Create a secure VPN with MFA to encrypt any form of communication between remote devices and internal networks. • Using encryption protocols like TLS/SSL • Implementing the least privilege principles. • Configuring firewalls to monitor and filter any inbound and outbound traffic
Mitigating Risk:	These controls will help protect its technological domain by securing remote access for its employees and data transmission. A VPN with MFA and TLS/SSL ensures encrypted, authorized connections, while implementing the least privilege and firewalls limiting access and blocking unauthorized traffic.

Vulnerability Four

Risk Domains:	People, Process, and Technology are all three crucial components because security issues arise when a single device connects to multiple networks, thereby increasing the risk of unauthorized access to sensitive data. And that "patients, guests, and employees are sharing the same device on the same network
Security Controls:	• **Creating a VLAN for employees, guests, and patients** • **Creating different networks for each group setting** • **Training employees on how to use the networks properly**
Mitigating Risk:	By separating all three networks, these controls reduce risks across all domains and prevent unauthorized access or data breaches.