1-2 Project One Stepping Stone: Risk Domain Analysis

Joshua Merren

Southern New Hampshire University

CYB-420-13227-M01 Enterprise Security

Professor Aaron Tyler

10 January 2025

I. Vulnerability One: Restricted Access

A. Explain which of the risk domains Vulnerability One exemplifies.

Vulnerability One falls under the "Technology" risk domain. Network delays and lost communications point to problems within the organization's technological infrastructure. These issues could stem from outdated or improperly configured hardware, such as the office router, switches, or hubs, or network congestion caused by high traffic. The vulnerability directly affects the technology's performance, leading to its categorization under this domain.

B. Implement security controls to mitigate the risk that is introduced by Vulnerability One.

To mitigate the risk, I recommend upgrading the current network equipment, such as replacing the standard four-port hub with a managed switch to improve data traffic management. Additionally, implementing Quality of Service (QoS) settings on the router can prioritize critical data like patient records over less important traffic. Regular maintenance, such as firmware updates and network monitoring tools, can ensure smoother operations and quicker identification of issues.

C. Assess how the implemented controls will be useful in mitigating risk for the security domain.

The root cause of delays and data synchronization issues is addressed through the suggested controls, with improvements made to the network's efficiency and reliability. Upgrading to a managed switch allows for better traffic management, reducing congestion and ensuring critical operations are not delayed. The prioritization of essential data is achieved through QoS, ensuring uninterrupted transmission of patient records and updates, which directly enhances the reliability of the technology domain.

II. Vulnerability Two: Physical Security Risks

A. Explain which of the risk domains Vulnerability Two exemplifies.

Vulnerability Two is part of the "Process" risk domain. Protecting physical assets like the examination rooms and back office requires implementing procedures and policies that control who has access. Without a straightforward process, sensitive areas and assets, such as stored medicine, could be misused or stolen. The absence of such controls creates the risk of accidental and intentional misuse of these critical assets, compromising operational efficiency and regulatory compliance.

B. Implement security controls to mitigate the risk that is introduced by Vulnerability Two.

To mitigate this risk, I recommend implementing physical security measures such as installing electronic locks on the back office and examination room doors, accessible only with keycards or codes. Assigning role-based access permissions ensures that only authorized personnel, such as doctors or administrators, can enter restricted areas. Adding surveillance cameras to monitor access and activity further enhances security. Additionally, keeping a digital log of access records can help track and review any unauthorized attempts to access these areas.

C. Assess how the implemented controls will be useful in mitigating risk for the security domain.

These controls provide a structured process for managing access to sensitive areas, ensuring only authorized individuals can enter. Role-based permissions reduce the risk of unauthorized access, and surveillance cameras act as both a deterrent and a tool for incident review. These measures create a more secure environment and align with compliance goals like HIPAA. Access logs can further help in auditing and identifying any unusual activity, making these controls comprehensive in addressing physical security risks.

III. Vulnerability Three: Remote Access Risks

A. Explain which of the risk domains Vulnerability Three exemplifies.

Vulnerability Three exemplifies the "People" risk domain. Allowing remote employees to access office resources introduces risks tied to how people interact with the system. Improper access management or lack of secure practices, such as weak passwords, could lead to breaches. These risks are compounded by the potential lack of employee awareness regarding secure remote work practices, making the human element a significant concern in this scenario.

B. Implement security controls to mitigate the risk that is introduced by Vulnerability Three.

I recommend implementing a Virtual Private Network (VPN) to address this risk and secure remote connections. All remote access should require multi-factor authentication (MFA) to ensure that only authorized users can connect. Training sessions for remote employees on secure practices, such as recognizing phishing attempts, would further reduce risks. Additionally, endpoint protection software on employee devices can detect and prevent malware or unauthorized activities during remote access.

C. Assess how the implemented controls will be useful in mitigating risk for the security domain.

Using a VPN encrypts remote communications, reducing the risk of data interception. MFA adds a layer of security by requiring additional verification beyond just a password. Employee training builds awareness and reduces the chances of human errors leading to security breaches, making the people domain more secure. Endpoint protection software enhances the overall security posture by monitoring and protecting devices used for remote work, addressing potential vulnerabilities introduced by end-user behavior.

IV. Vulnerability Four: Shared Device Risks

A. Explain which of the risk domains Vulnerability Four exemplifies.

Vulnerability Four falls under the "Technology" risk domain. Sharing a single device for patient/guest and employee access creates a significant technological risk due to the lack of network segmentation, which could lead to unauthorized access and data breaches. This scenario highlights a failure to properly isolate network traffic, which is critical for maintaining confidentiality and integrity in a healthcare environment.

B. Implement security controls to mitigate the risk that is introduced by Vulnerability Four.

I recommend creating separate networks for employees and guests using a VLAN (Virtual Local Area Network) to mitigate this vulnerability. Implementing a firewall to monitor and control traffic between these networks ensures that sensitive office data remains secure. Providing dedicated devices for guests and employees would further separate access points. Applying strict ACLs (Access Control Lists) on the router can also block guest traffic from accessing sensitive internal resources.

C. Assess how the implemented controls will be useful in mitigating risk for the security domain.

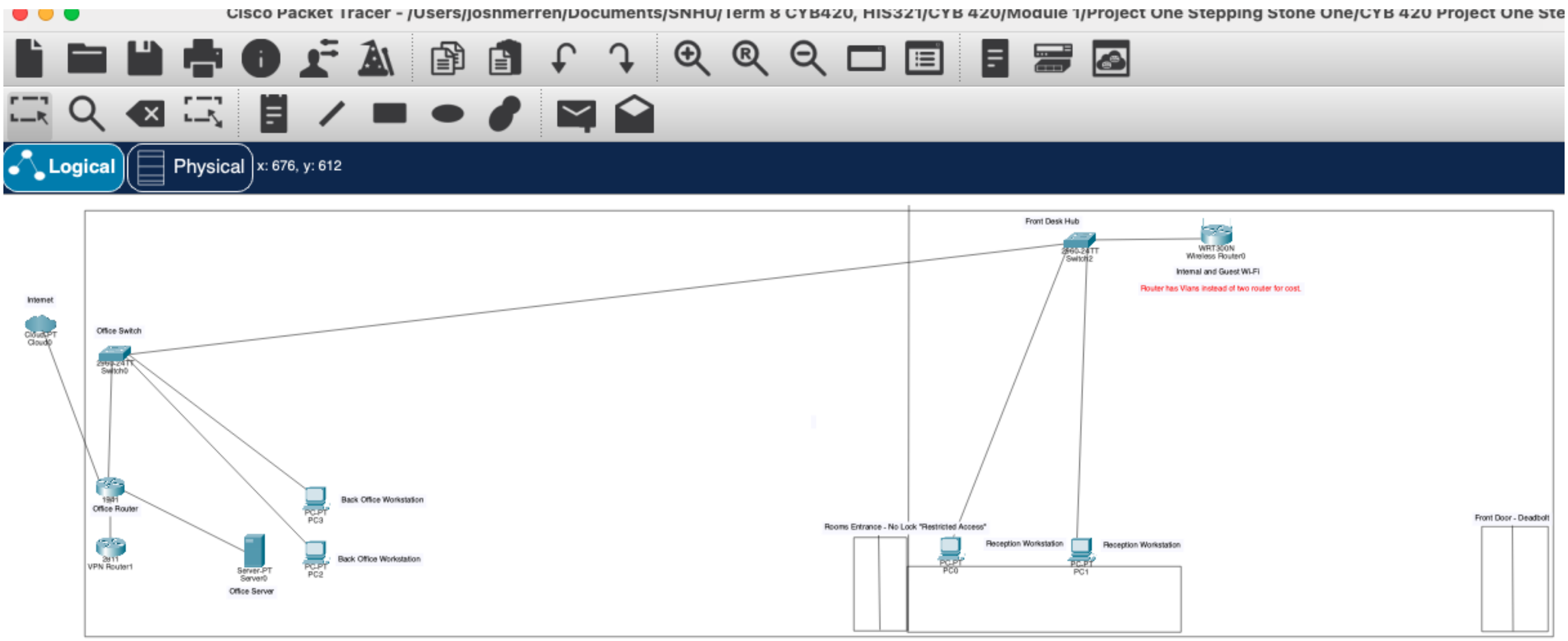
I recommend creating separate networks for employees and guests using a VLAN (Virtual Local Area Network) to mitigate this vulnerability. Implementing a firewall to monitor and control traffic between these networks ensures that sensitive office data remains secure. Providing dedicated devices for guests and employees would further separate access points. Applying strict ACLs (Access Control Lists) on the router can also block guest traffic from accessing sensitive internal resources.

V. Adversarial Mindset:

A. Explain how you used your adversarial mindset to help inform your decisions.

An adversarial mindset was employed by considering the perspective of a potential attacker to identify ways in which vulnerabilities might be taken advantage of. For example, I considered how poor network segmentation could allow unauthorized access to sensitive data or how a lack of physical security could lead to theft. This approach helped me recommend specific controls that address obvious and subtle risks, ensuring a comprehensive security strategy. By analyzing each vulnerability from multiple perspectives, I was able to propose solutions that align with best practices and reduce the overall risk to the organization. Additionally, by considering the motivation and tools an attacker might use, I focused on mitigating risks that pose the highest threats to the organization's operations and compliance requirements.

Screenshot:



In the diagram, I have added VLANs to the internal and guest routers, as it is more cost-saving to do VLANs instead of a separate router. I also added a 2811 router to the office network for VPN remote access. I also included labels on the entrance for restricted access for physical security. I would also add cameras to the doorways and swipe access.