SECURE NETWORK DESIGN – D482

DHN1 TASK 1: Network Merger and Implementation Plan

Shane M. Deitle

Western Governors University

A. Describe two current network security problems and two current infrastructure problems for each company:

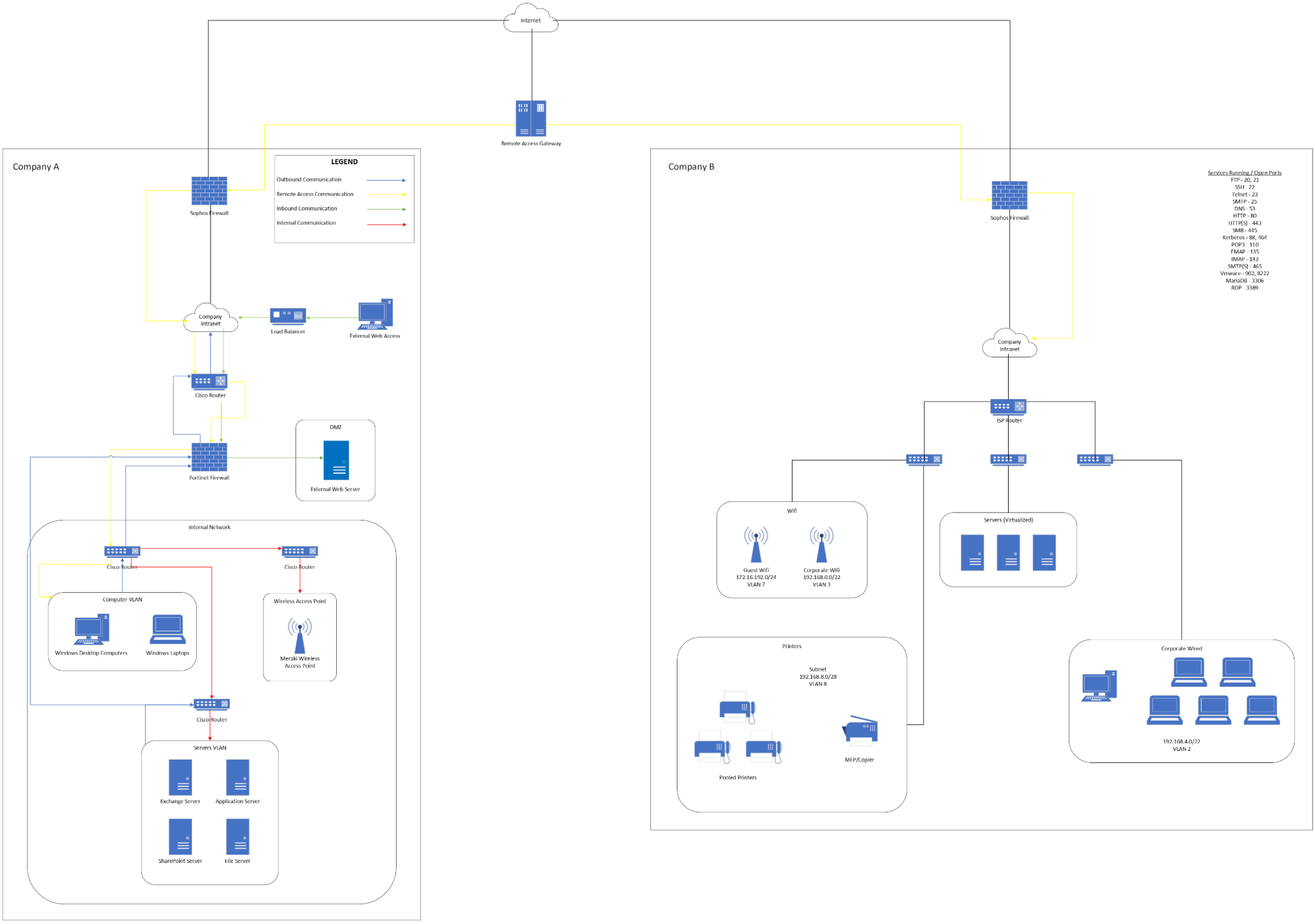
- Network Security Problems:
  - Company A:
    1. Limited Password Complexity: Company A has a network security problem pertaining to its weak password policies. All users are currently using eight-character passwords, which are easily cracked and pose a significant security risk.
    2. Open Ports: Company A has open ports 21-90 and 3389, which can be used as vulnerabilities in an attack. This introduces a high risk of the network being accessed without proper authorization.
  - Company B:
    1. Multiple Critical Vulnerabilities: Company B is exposed to several critical vulnerabilities, such as Distributed Ruby (dRuby/DRb) Remote Code Execution and Java RMI Server Insecure Default Configuration. A high security risk to the network is introduced by these vulnerabilities.
    2. Lack of MFA Enforcement: Company B is not enforcing Multi-Factor Authentication (MFA) across all users, leading to a high security risk, as it can result in unauthorized access to critical systems.
- Infrastructure Problems:
  - Company A:
    1. End-of-Life Equipment: Company A is using end-of-life equipment. This infrastructure problem does not introduce an immediate high risk but will need to be addressed to ensure long-term sustainability, as well as maintaining network security.
    2. Unused User Accounts: Company A does not routinely remove user accounts that are not in use anymore. This practice poses a moderate risk as these accounts can be exploited for unauthorized access.
  - Company B:
    1. End-of-Life Detection: Company B's network has systems with operating systems that have reached their End of Life (EOL). While the probability of this infrastructure problem being taken advantage of is low, addressing this is crucial for long-term security.
    2. Weak Passwords and Open Ports: Company B faces issues with weak passwords and open ports, such as PostgreSQL weak passwords and FTP Brute Force Logins. These infrastructure problems introduce a moderate to high risk to security and need attention immediately.

B. By analyzing the given network diagram and vulnerability scan for both companies, describe two existing vulnerabilities for each company and explain the impact, risk, and likelihood associated with each described vulnerability:

- Company A:
  1. Open Ports
     - Description: Company A has open ports 21-90 and port 3389, making it vulnerable to unauthorized access and potential attacks.
     - Impact: If this vulnerability is exploited, it may lead to potential damage to critical systems, data breaches, and unauthorized access.
     - Risk: High, as the open ports expose the network to severe security risks.
     - Likelihood: High, as open ports are attractive targets for attackers.
  2. Weak Passwords
     - Description: All users in Company A are restricted to eight-character passwords, which are easily cracked.
     - Impact: This vulnerability could lead to potential disturbance of services, unauthorized access, and possible data breaches.
     - Risk: High, as weak passwords pose a significant threat to network security.
     - Likelihood: High, as attackers often target weak passwords.
- Company B:
  1. Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities
     - Description: Multiple remote code execution vulnerabilities in Distributed Ruby (dRuby/DRb) expose Company B to the risk of unauthorized code execution.
     - Impact: Exploitation of these vulnerabilities can result in a root-level compromise of servers or infrastructure devices (Britt, n.d.).
     - Risk: High, as these vulnerabilities are critical and pose a severe threat to organizational operations and assets.
     - Likelihood: High, as critical vulnerabilities are attractive targets for attackers.
  2. Lack of MFA Enforcement
     - Description: Company B does not ensure all of its employees use Multi-Factor Authentication (MFA), this can increase the risk of access by unauthorized parties.
     - Impact: This vulnerability could result in unauthorized access to critical systems and potential loss of data.
     - Risk: High, as the lack of MFA poses a significant risk to security.
     - Likelihood: High, as attackers may exploit this weakness.

C. Create a network topology diagram with details of the proposed merged network requirements:

1. Remote Access Communication:
   - Employees of both Company A and Company B can access the network securely via a centralized Remote Desktop Gateway, which ensures secure remote access.
2. Inbound Communication:
   - External web access is managed through a load balancer that distributes traffic to the DMZ (External Web Server), which will enhance security as well as availability.
3. Internal Communication:
   - Internal communication within the merged network is facilitated by a combination of Cisco switches, ensuring efficient and secure data transfer.
4. Servers VLAN:
   - This VLAN includes servers from both companies, such as the Exchange Server, Application Server, SharePoint Server, File Server, and virtualized servers from Company B.
5. Computer VLAN:
   - This VLAN is dedicated to Windows desktop computers, laptops, and workstations used by employees from both companies.
6. Wired and Wireless Access:
   - The merged network includes wired and wireless access points to cater to the diverse needs of employees, with Meraki Wireless Access Points ensuring secure Wi-Fi access.
7. Firewall and Security:
   - The network is protected by a powerful Fortinet Firewall that filters traffic, enhances security, and enforces security policies.
8. Cloud Integration:
   - The merged network supports cloud integration to leverage the scalability and redundancy offered by cloud services. A cloud-based security solution will help further enhance protection from attacks (Intel, n.d.).


Internet
Remote Access Gateway
Company A
LEGEND
Outbound Communication
Remote Access Communication
Inbound Communication
Internal Communication
Sophos Firewall
Company Intranet
Load Balancer
External Web Access
Cisco Router
DMZ
Fortinet Firewall
External Web Server
Internal Network
Cisco Router
Cisco Router
Computer VLAN
Windows Desktop Computers
Windows Laptops
Wireless Access Point
Meraki Wireless Access Point
Cisco Router
Servers VLAN
Exchange Server
Application Server
SharePoint Server
File Server
Company B
Sophos Firewall
Services Running / Open Ports
FTP - 20, 21
SSH - 22
Telnet - 23
SMTP - 25
DNS - 53
HTTP - 80
HTTP(S) - 443
SMB - 445
Kerberos - 88, 464
POP3 - 110
RPAP - 135
IMAP - 143
SMTP(S) - 465
Vmware - 902, 8222
MariaDB - 3306
RDP - 3389
Company Intranet
ISP Router
Wifi
Guest Wifi
172.16.102.0/24
VLAN 7
Corporate Wifi
192.168.0.0/22
VLAN 3
Servers (Virtualized)
Printers
Subnet
192.168.8.0/28
VLAN 8
Pooled Printers
MFP/Copier
Corporate Wired
192.168.4.0/22
VLAN 2

D. Identify the layer for all components in the topology diagram referencing the layers of the OSI model and TCP/IP protocol stack:

Component	OSI Model	TCP/IP Protocol
Remote Access Gateway	Layer 3 (Network)	Internet
Load Balancer	Layer 4 (Transport)	Transport
DMZ (External Web Server)	Layer 7 (Application)	Application
Cisco Switches	Layer 2 (Data Link)	Network Access
Servers VLAN	Layer 3 (Network)	Internet
Computer VLAN	Layer 2 (Data Link)	Network Access
Wired and Wireless Access Points	Layer 2 (Data Link)	Network Access
Fortinet Firewall	Layer 7 (Application)	Application
Cloud Integration	Multiple Layers	Multiple

(Williams, 2023)

E. Explain the rationale for adding, deleting, or repurposing network components in the newly merged network topology diagram:

1. Remote Access Gateway:
   - Rationale for Adding: This component is essential to provide secure remote access for employees from both companies. A remote access gateway ensures that employees can work efficiently from either location, or even remotely.
   - Budgetary Constraints: The remote access gateway aligns with the budget as it enhances productivity while ensuring data security.
2. Load Balancer:
   - Rationale for Adding: The load balancer is introduced to improve the availability and security of external web access, distributing traffic to the DMZ efficiently.
   - Budgetary Constraints: The load balancer is an essential investment to ensure high availability and security of the web services.
3. DMZ (External Web Server):
   - Rationale for Keeping: The DMZ houses the external web server, providing a secure location for web services and protecting the internal network from external threats.
   - Budgetary Constraints: No added budgetary costs, existing equipment.
4. Cisco Switches:
   - Rationale for Keeping: Cisco switches play a vital role in internal communication within the merged network. They are already part of Company A's network and will be retained.
   - Budgetary Constraints: No additional investment is required.
5. Servers VLAN:
   - Rationale for Keeping: This VLAN contains critical servers from both companies, it is essential to ensure the integrity of this VLAN and not repurpose it.
   - Budgetary Constraints: Existing hardware will be utilized, minimizing additional costs.
6. Computer VLAN:
   - Rationale for Keeping: The computer VLAN serves the desktop computers and laptops for both companies. Keeping the computer VLAN will aid in supporting daily operations.
   - Budgetary Constraints: No additional investment is required.
7. Wired and Wireless Access Points:
   - Rationale for Keeping: Access points ensure connectivity for both wired and wireless devices. They will be retained and optimized for performance.
   - Budgetary Constraints: Optimization of existing equipment is a cost-effective approach.
8. Fortinet Firewall:
   - Rationale for Keeping: The Fortinet Firewall provides protection for the network. It also falls in line with the security principles of the newly proposed, merged network.
   - Budgetary Constraints: The firewall is a necessary security component and is budgeted accordingly.
9. Cloud Integration:
   - Rationale for Adding: Cloud integration is introduced to enhance scalability and redundancy. Cloud integration was pointed out to be an interest to the executives.
   - Budgetary Constraints: The cloud integration is well within the budget and enhances network capabilities.

F. Explain two secure network design principles that are used in the proposed network topology diagram:

1. Defense in Depth:
    - Explanation: Defense in Depth is a fundamental network security principle that involves layering security measures to provide multiple levels of protection. In the proposed network topology, this principle is implemented by having multiple layers of security controls, such as firewalls, access controls, and encryption, at various points in the network.
    - Application in the Network: The Fortinet Firewall, used in Company A, serves as an example of implementing Defense in Depth. The firewall acts as a barrier between the internal network and the external web services, improving security by inspecting and filtering traffic at the perimeter of the network.
2. Least Privilege Access:
    - Explanation: The Least Privilege Access principle revolves around granting individuals or systems the minimum levels of access and permissions needed to perform their tasks. In the proposed network, the principle of least privilege is applied to user accounts and system access controls to reduce the attack surface and limit potential breaches.
    - Application in the Network: Network components like the Remote Access Gateway are configured to enforce the principle of Least Privilege Access. Remote users are granted access only to specific resources they need, and they do not have excessive permissions that could be exploited by attackers.

G. Explain how the proposed merged network topology diagram addresses two regulatory compliance requirements that are relevant to the newly merged company:

1. Health Insurance Portability and Accountability Act (HIPAA):
    - Relevance: HIPAA is relevant to the Company B's involvement in the freshly merged company, as it handles sensitive patient information from the medical providers it deals with. Protecting the confidentiality and integrity of patient data is a must for the network to fulfill HIPAA regulations (Cole, 2022).
    - Addressing Compliance: The proposed network topology design includes a dedicated DMZ (External Web Server) to ensure that external web services, which may handle patient data, are securely separated from the internal network. This segregation helps by preventing access to sensitive information by unauthorized parties.
2. Payment Card Industry Data Security Standard (PCI DSS):
    - Relevance: PCI DSS is relevant to both companies, and in turn the newly merged company, as the company will accept credit cards and deal with financial transactions. PCI DSS compliance is necessary to protecting credit card data and maintaining the trust of the customers (Cole, 2022).
    - Addressing Compliance: The proposed network topology design includes security measures to protect payment processing systems and servers. By implementing strong access controls and encryption measures within the network, the merged company can ensure that credit card data is handled in a safe and protected manner.

H. Describe two emerging threats that are appliable to the merged organization

1. Zero-Day Exploits:
    - Network Security Risks: Zero-day exploits refer to vulnerabilities in hardware or software that are discovered and exploited by cyber attackers before developers can release a fix (patch). If a zero-day exploit is leveraged against the merged network, it can result in unauthorized access, data breaches, and service disruptions. Since Company A deals with the financial industry and Company B handles medical data, both have valuable targets that cybercriminals might be interested in exploiting.
    - Performance Impacts: Mitigating zero-day exploits often involves applying security patches quickly, which can lead to frequent software updates. This can impact network performance, which is especially bad for critical systems that cannot be down for extended or any periods of time. Careful planning will be needed to implement rapid patch deployment while minimizing disruptions to the network.
    - Risk Management: To mitigate the risk of zero-day exploits, the merged company should implement robust intrusion detection and prevention systems (IDS/IPS), threat intelligence feeds, and timely patch management processes. Regular vulnerability canning/assessments and security awareness training for employees are also crucial steps in the process of identifying and mitigating these threats.
2. AI-Powered Attacks:
    - Network Security Risks: Artificial intelligence-powered attacks are becoming more sophisticated, using machine learning to adapt and evade traditional security measures. These attacks are able to target vulnerabilities within the network, launch advanced phishing campaigns towards employees, and infiltrate systems without any sign of detection. As the merged organization seeks to implement cloud-based technologies and expand its footprint, these evolving threats may be more likely to attack it.
    - Performance Impacts: Implementing AI-driven security measures to combat AI-powered attacks can consume significant network resources and processing power. If not properly dealt with, these attacks can affect network performance as well as response times.
    - Risk Management: To mitigate AI-powered attacks, the merged company should invest in AI-driven security solutions capable of identifying and responding to these advanced threats. Regular AI-based threat analysis and security training are essential to keep pace with evolving attack tactics.

I. Summarize your recommendations for implementation of this proposed merged network based on the scenario and budgetary requirements:

Cost-Benefit Analysis:

1. On-Premises Infrastructure:
    - Benefits: Keeping some on-premises infrastructure offers full control over certain data and applications. This is crucial for regulatory compliance and security and is especially true for financial and healthcare data. On-premise infrastructure can also provide low-latency access to important systems.
    - Costs: The initial investment costs for the hardware and software of on-premises infrastructure can be high (Team Cleo, n.d.). Ongoing maintenance costs, security costs, and energy costs are other factors to keep in mind.
2. Cloud-Based Infrastructure:
    - Benefits: Moving some infrastructure to cloud-based solutions provide both scalability and flexibility, making it easier to adapt to the merged organization's needs as they change. Cloud-based solutions can also offer better capabilities for redundancy and disaster recovery (Intel, n.d.). Additionally, cloud solutions can help optimize costs and limit wasted/unused resources by paying for only what is currently needed.
    - Costs: While cloud solutions offer initial cost savings in terms of infrastructure and maintenance, ongoing subscription costs can begin to rise. This is especially true while the newly merged business is adapting, changing, and growing.

Recommendations and Justification:

- Hybrid Cloud Approach: This approach combines on-premise infrastructure as well as cloud infrastructure to achieve a balance between control, security, and cost-effectiveness. It also fits well with the given budget of $50,000 in the first year. Critical and sensitive systems, such as those handling financial and healthcare data, should be kept on-premises, while non-sensitive systems can be moved to the cloud for potential cost savings and resource scaling (Team Cleo, n.d.).
- Cloud Security Measures: Invest a portion of the budget in robust cloud security solutions and services to protect cloud-based resources. To ensure the security of applications and data that are hosted on the cloud, implement data encryption, identity and access management, and continuous monitoring.
- Comprehensive Training: Allocate resources for comprehensive cybersecurity training for all employees. Security awareness and education are very important to preventing common threats, such as phishing and social engineering.
- Regular Auditing and Testing: Establish a continuous auditing and testing schedule to ensure that the network remains secure and compliant with regulatory requirements. Regular vulnerability assessments and penetration testing should be part of the strategy.

J. Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased, or summarized.

Williams, L. (2023, October 28). *TCP/IP vs OSI Model – difference between them*. Guru99. https://www.guru99.com/difference-tcp-ip-vs-osi-model.html

Intel Corporation. (n.d.). *What is hybrid cloud? benefits and use cases*. Intel. https://www.intel.com/content/www/us/en/cloud-computing/what-is-hybrid-cloud.html

Team Cleo. (n.d.). *Blog: On premise vs. cloud: Key differences, benefits and risks*. Cleo. https://www.cleo.com/blog/knowledge-base-on-premise-vs-cloud

Britt, J. (n.d.). *Module: DRb (Ruby 1.9.3)* . Ruby-doc.org. https://ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html

Cole, B. (2022, June 9). *What is Regulatory Compliance?*. CIO. https://www.techtarget.com/searchcio/definition/regulatory-compliance