Risk-Based Approach to Organizational Network Integration

Elijah Olson

Western Governors University

D482 Secure Network Design

Introduction

The merger of Company A, a financial industry company, with Company B, a leader in medical software, presents numerous challenges. Each company faces different regulatory compliance requirements and unique needs for network and infrastructure makeup. This report aims to identify deficiencies in each company's network and infrastructure, pinpoint vulnerabilities, and provide recommendations for creating a cohesive and secure network design within the budgetary constraints provided.

Network Security and Infrastructure Problems

Company A Network Security and Infrastructure Problems

Infrastructure

Currently, Company A is utilizing multiple servers running Windows server 2012 and Windows server 2012R2 both of which have well exceeded their end-of-life support dates. Both systems had their extended support dates end October 10, 2023 (Microsoft, n.d.). This poses a significant risk to the organization because critical security patches and updates will not be released when new vulnerabilities are discovered.

Within Company A's network topology there are no redundancies for system failures. There are currently multiple single points of failure for data transmission on the network. In the present design if any system outage were to be experienced then there would be total work stoppages until the affected system was restored.

Network

Company A utilizes four Cisco 3750X model network switches at various points in its topology, this hardware reached end of life with last date for maintenance releases of September 4, 2024 (*End-of-Sale and End-of-Life Announcement for the Cisco Catalyst 3750-X Series Switches*, 2023). While still able to receive support from Cisco, they are not releasing any security patches or updates for these models exposing the organization to potential vulnerabilities.

Within the network topology a Cisco 7600 router is being utilized, all support for this asset ended June 30, 2021 (*End-of-Sale and End-of-Life Announcement for the Cisco Service and Application Module for IP (SAMI) Hardware and Wireless Security Gateway Software for the Cisco 7600 Series Routers*, 2015). As previously identified, lack of support surrounding security patches and updates opens the organization to another vulnerability.

Company B Network Security and Infrastructure Problems

Infrastructure

Company B currently provides no support and relies exclusively on third-party infrastructure and support. To further complicate matters multiple vendors are utilized creating the potential for multiple points of security failure. This exposes Company B to a high risk of threats being introduced not via Company B itself but through a vendor system into Company B's network.

Windows XP and Windows 7 are still being utilized on workstations within the network. Windows XP support ended April 8, 2014 (Microsoft, n.d.-b) and Windows 7 had support ended January 14, 2020 (Microsoft, n.d.-a). In addition to security risk implications of running outdated software, there is potential that this will place Company B out of regulatory compliance standards.

Network

Multi-factor authentication (MFA) is the process of verifying your identity utilizing more than one means of verification. The three most utilized systems for identity verification in MFA are: something you know, something you have, and something you are (Microsoft, 2024). Requiring MFA increases access security to organizational resources, currently Company B does not enforce this policy across all users. By arbitrarily applying an MFA policy to access organizational resources the company is opening themselves up to security risk and potentially regulatory violations.

All users have local administrative privileges on workstations configured for Company B's network. This allows standard end users the ability to modify system configurations with the potential to introduce a vulnerability to the network. This further opens Company B to security risk and potential regulatory compliance violations.

Existing Vulnerabilities

Company A

According to CISA employing strong password policies and best practices can reduce the attack surface by reducing the risk of credential-based attacks (CISA, 2025). The policies currently in place only require eight-character passwords without complexity requirements that meet industry best practices. The threat posed to Company A by these insufficient password requirements introduces a high risk of a credential-based attack. The likelihood of a credential-based attack impacting the organization is high as dictionary and brute force attacks occur with increasingly regularity. The impact on the organization would be devastating, with the large amount of personally identifiable information Company A stores for customers, a breach would open the organization up to civil, regulatory, and reputational damages.

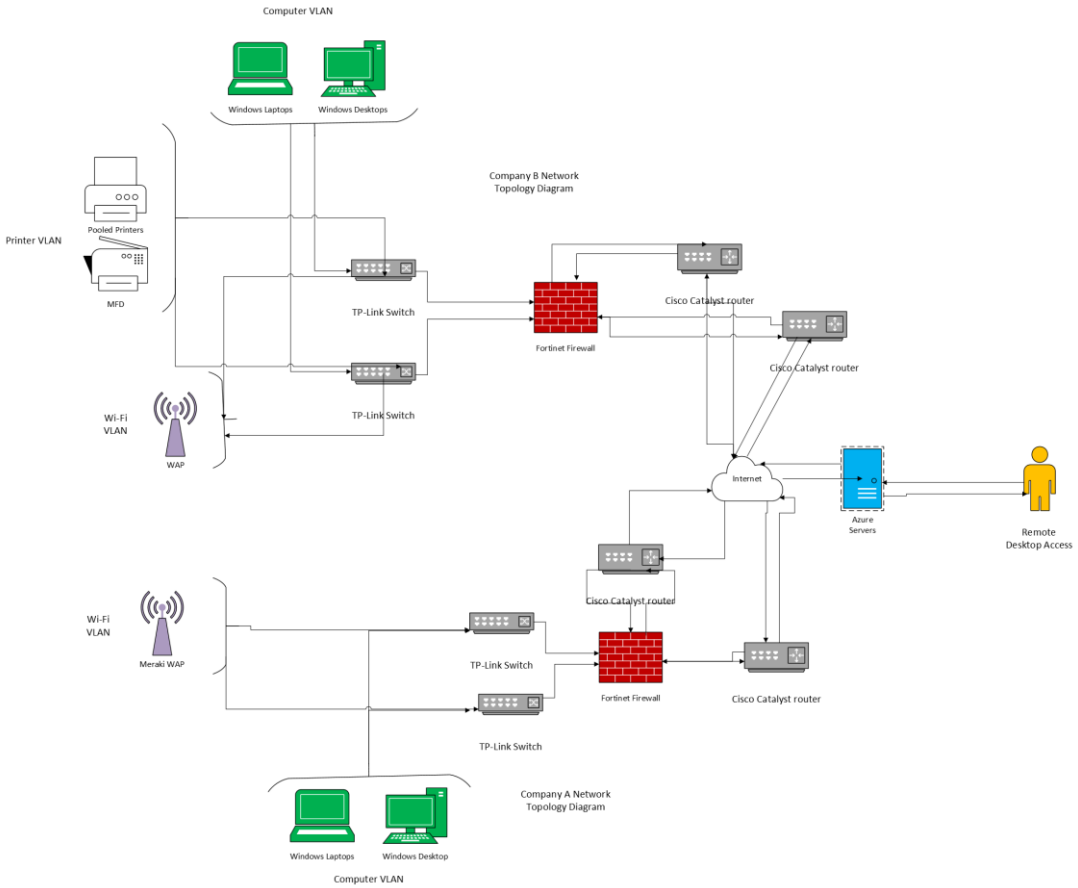
Another potentially damaging user account issue identified is that user accounts no longer in use are not removed from systems. By maintaining deprecated user accounts active on company systems, the organization is increasing the available attack surface. The potential for unauthorized access to the system introduces the ability for personal data to be compromised causing non-compliance with regulations. Additionally, the impact on the organization's reputation if exposed would cause a loss of confidence in Company A. The likelihood of this threat occurring is moderate, attackers frequently scan systems for known credentials and stale accounts frequently have weaker passwords. The risk to the organization of maintaining unused accounts opens the organization to a moderately high level of risk.

Company B

The lack of MFA enforcement across all user accounts opens the potential for unauthorized access to system resources including the potential for confidential information to be exposed. This is especially important for this organization as it works with personal health information (PHI) which is governed by HIPAA compliance requirements. User accounts without MFA enforced have the potential to be compromised by credential-based attacks such as brute-force password attacks. The likelihood that an account without MFA enabled being compromised is high.

The audit of company systems shows FTP Brute Force Logins vulnerability to network systems. The FTP servers have the potential for confidential and personally identifiable information being exposed. There is also the possibility that attackers could introduce malicious files to the FTP server, further infecting the system. The direct implications involve regulatory compliance violations and reputational harm. The likelihood that this vulnerability could be exploited is high due to the weaker security protocols utilized by FTP.

Integrated Network Topology



System Components

Device	OSI Layer	TCP/IP Layer
Azure Servers	Application (Layer 7)	Application
Router	Network (Layer 3)	Internet
Firewall	Application (Layer 7)	Application
Wireless Access Points	Data Link (Layer 2)	Network Interface
Laptops & Workstations	Application (Layer 7)	Application
Printers	Application (Layer 7)	Application
Cabling	Physical (Layer 1)	Network Interface
VPN	Network (layer 3)	Internet
Switches	Data Link (Layer 2)	Network Interface

Recommended Network Integration Plan

Recommended System Upgrades			
Device	**Quantity**	**Unit Price**	**Total Price**
Azure cloud servers	1	$20,000.00	$20,000.00
Azure IAM	1	$2,000.00	$2,000.00
Azure VPN Gateway	1	$5,000.00	$5,000.00
Azure Security Center	1	$1,000.00	$1,000.00
Azure Monitor	1	$3,000.00	$3,000.00
Cisco Catalyst C8200L-1N-4T	4	$1,000.00	$4,000.00
TP-Link JetStream 24-Port switch	4	$300.00	$1,200.00
FortiGate 200F series firewall	1	$4,000.00	$4,000.00
Microsoft Sentinel SIEM	1	$4,000.00	$4,000.00
Total Investment			**$44,200.00**

The decision to purchase four Cisco Catalyst routers and four TP-Link switches was for multiple reasons, the first is that Company B was utilizing third-party devices for their infrastructure needs therefore the decision to purchase dedicated equipment for this location was made. The equipment at the Company As location was replaced due to current hardware having exceeded end of life support windows, which poses a security risk. Two routers and two switches were purchased for each location to provide redundancy that both locations were previously lacking.

Company A has been utilizing a FortiGate 800D series firewall which is still receiving support from the vendor so upgrading this firewall can be accomplished in future years. Company B was utilizing two Sophos XG firewalls which reached the end of life in March of 2025 (Maronda, 2025). The lack of vendor support poses a potential security vulnerability; therefore, the decision was made to purchase a FortiGate 200F series firewall to replace them.

With an organizational focus to implement cloud-based solutions during this merger the following solutions were selected: Azure cloud servers, Azure Identity and Access Management services, Azure VPN Gateway, Azure Security Center, Azure Monitor, and Microsoft Sentinel SIEM. The decision to utilize funds for these services would replace the deprecated on-premises servers being used by shifting data storage and management to the cloud. This also aids in the newly acquired work location with Company B to more easily access necessary organizational resources. The additional services selected allow Company A's Information Technology management teams to administer user access for individuals located at Company B site. The products also provide essential security and event management services to aid in network security.

The decision to repurpose existing laptops and workstations was made due to the prioritization of migrating essential infrastructure to a cloud environment within budgetary constraints. While some of these assets are utilizing older operating systems that have moved past the end of support windows, the threat posed by these outdated operating systems are able to be mitigated by security solutions that were selected. The recommendation is that non-essential laptops and workstations running outdated operating systems be replaced in future budget years.

Additionally, at both work sites the decision was made to continue utilizing existing wireless access points (WAPs) rather than replace them at this time. Currently the WAPs in place are within support windows for vendor updates. In future budgets as the individual WAP approaches the end-of-life date I would recommend upgrading at that time.

Principles of Design

In redesigning Company A and Company B's networks to merge them into one cohesive system the following secure network design principles were utilized: network segmentation and strong authentication. To reduce the impact of a network security breach, the network is broken into separate VLANs to reduce the likelihood that an attacker can easily move across organizational systems. Requiring the use of strong authentication methods via enforcement of MFA for all users verifies identity prior to allowing access to company resources. This is especially important with the migration to cloud-based services and remote workers utilizing a VPN.

Regulatory Compliance Concerns

With Company A operating in the financial industry and Company B operating in the health care sector individual compliance needs were considered and provided some overlap between regulatory requirements. As an organization in the financial sector Company A is required to comply with the Sarbanes-Oxley Act (SOX). SOX requires companies to maintain sufficient internal controls and safeguards for financial data (AuditBoard, 2025). The proposed network addresses this with firewalls, cloud-based security center, monitor, and SIEM. This multistep approach ensures that access to financial data is only accessible to authorized parties.

This acquisition of Company B requires that both organizations are compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) including the newer amendment with the Health Information Technology for Economic and Clinical Health (HITECH) Act. Company B provides specialized software to medical providers and therefore must ensure they are safeguarding any Personal Health Information (PHI) collected, stored, or transmitted within their systems (*Summary of the HIPAA Security Rule*, 2024). By utilizing MFA before providing access to organizational resources, the proposed network secures individual's electronic PHI utilized by the companies.

Potential Threats

One emerging threat posed to the organization is the increased frequency of environmental disasters causing outages to critical infrastructure. By migrating essential servers to a cloud-based model, redundancy is provided by design with cloud infrastructure including multiple geographic locations for the data centers housing the servers. This reduces the impact an outage occurring at a single worksite has on the business because essential resources would still be available to the other location and remote workers.

Another emerging threat with the potential to impact operations is ransomware which is defined by the F.B.I. as a form of malicious software that prevents access to files, systems, or networks with the demand that a ransom be paid for restored access being granted (FBI, n.d.). By migrating data from onsite to cloud-based servers the risk is shifted from the companies directly to the cloud service provider for data previously stored in onsite servers. This reduces the impact a potential ransomware attack would have on individual sites because the essential data is housed at a cloud-based vendor which have additional security protocols to mitigate ransomware attacks.

Cost-Benefit Analysis

The proposed network realignment to merge Company A and Company B focuses on cloud services implementation with year one budgetary aim at migrating data to cloud systems. The elimination of on-premises servers reduces infrastructure maintenance costs related to physical server hardware, reduced ongoing operating costs at Company A's location such as reduced electricity consumption and lower heating and cooling costs. An additional benefit is that space previously utilized by the servers can be repurposed into additional workspace. The migration to cloud also reduces the attack surface to the organization and the potential lost revenue experienced by a breach.

An additional benefit to investing in cloud integration is the scalability presented versus maintaining on-premises servers. As illustrated through the acquisition of Company B, this organization has increased growth

opportunities with the potential to expand into other sectors. The initial investment in migrating data to cloud-based services allows for ease of continued growth and scalability of data resources dynamically.

Conclusion

The challenges presented through Company A's merger with Company B surrounding regulatory compliance, unique network and infrastructure design, and initial budget have been addressed in a cost-effective approach prioritizing ease of integration with cloud-based services. Vulnerabilities presented through outdated hardware and ineffective systems have been addressed to strengthen the security posture post-merger. The proposed network design plan provides opportunities at both sites for continued growth and further expansion into cloud-based solutions in the future.

References

AuditBoard. (2025). *What is SOX Compliance? 2025 Complete Guide | AuditBoard*. AuditBoard; What is SOX Compliance? 2025 Complete Guide | AuditBoard. https://auditboard.com/blog/sox-compliance

CISA. (2025). *Require Strong Passwords*. Www.cisa.gov. https://www.cisa.gov/secure-our-world/require-strong-passwords

End-of-Sale and End-of-Life Announcement for the Cisco Catalyst 3750-X Series Switches. (2023, March 7). Cisco. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-x-series-switches/catalyst-3750-x-series-switches-eol.html

End-of-Sale and End-of-Life Announcement for the Cisco Service and Application Module for IP (SAMI) Hardware and Wireless Security Gateway Software for the Cisco 7600 Series Routers. (2015, December 11). Cisco. https://www.cisco.com/c/en/us/products/collateral/wireless/7600-wireless-security-gateway/eos-eol-notice-c51-736397.html?dtid=osscdc000283&linkclickid=srch

FBI. (n.d.). *Ransomware*. Retrieved August 7, 2025, from https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

Maronda, S. (2025, April 22). *Sophos XG Firewall End of Life – Upgrade to Sophos XGS for Enhanced Network Security and Performance - Cloud Productivity Solutions*. Cloud Productivity Solutions. https://cloudproductivity-solutions.com/sophos-xg-firewall-end-of-life/

Microsoft. (n.d.-a). *Windows 7 - Microsoft Lifecycle*. Learn.microsoft.com. Retrieved August 6, 2025, from https://learn.microsoft.com/en-us/lifecycle/products/windows-7

Microsoft. (n.d.-b). *Windows Server 2012 - Microsoft Lifecycle*. Learn.microsoft.com. Retrieved August 6, 2025, from https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2012

Microsoft. (n.d.-c). *Windows XP - Microsoft lifecycle*. Learn.microsoft.com. Retrieved August 6, 2025, from https://learn.microsoft.com/en-us/lifecycle/products/windows-xp

Microsoft. (2024). *What is: Multifactor Authentication*. Support.microsoft.com. https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661

Summary of the HIPAA Security Rule. (2024, December 30). U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html