Task 1: Network Merger and Implementation Plan

By : Jordan Biggs

Part A:

Company A: Network Security Problems.

Company A is no longer required to remove user accounts. This issue causes a problem because it poses the risk that ex-employees will still access the system. These ex-employees could have malicious intent and cause damage to the systems or leak company data with their access. Revoking users' accounts when they are no longer needed eliminates this risk. Company A can also perform regular audits to find and delete unused users. Company A's second network security issue is granting all the users local admin rights. Company A is now a violation of the principle of least privilege and has the potential for an insider to use their elevated privilege to damage the system. Company A should only allow users access based on their respective roles to combat this issue.

Company A Infrastructure Problems

Company A has ports 21 - 90, 3389 open. This is an infrastructure problem because these open ports provide a gateway into your system that can be exploited. More infrastructure problems for company A would be the outdated operating systems (Windows 7, Windows Server 2012, and Windows Server 2012R2). These operating systems no longer have support, making them susceptible to new vulnerabilities and bugs.

Company B: Network Security Problems.

Company B currently allows all users to have local administrative privileges. This violates the principle of least privilege and risks an insider abusing their elevated privilege. A solution to this issue would be allowing users access based on their respective roles. Another network security problem is MFA not being enforced on all users. This threatens to violate confidentiality by possibly allowing an unauthorized user to access the system.

Company B Infrastructure Problems

Company B uses outdated operating systems no longer supported by Microsoft (Windows 7, Windows XP). Company B also has a poor FTP server configuration, which exposes its open services to the network.

Part B:

Company A

B1:

Company A has End-of-Life Equipment in use. Company A runs outdated operating systems, specifically Windows 7 & Windows Server 2012/2012R2. The manufacturer no longer supports these older versions,

so they've stopped receiving updates. These vulnerable systems are highly susceptible to malware, exploits & even APTs. Company A also has several open ports. These ports include 21-90 & 3389. Leaving these ports open exposes Company A & increases its attack surface. Port 3389 is a common target for brute-force attacks and ransomware, & leaving this port open is very dangerous.

B2:

Vulnerablities	**Impact**	**Risk**	**Likelihood**
Open port 21-90, 3389	If exploited, an open port can give attackers unauthorized access to systems. This can lead to the installation of malware or the disruption of services.	The risk is high because these unnecessary open ports can grant attackers direct access to critical services.	The likelihood is high because attackers frequently scan for open ports & try to exploit them, especially for port 3389.
End-of-Life Equipment	If exploited, attackers could gain unauthorized access, install malware, or even disrupt services.	The risk is high because if compromised, systems that handle sensitive data can lead to financial & reputational loss.	The likelihood is low because it is unlikely that the attackers will know that company A is using these old systems.

Company B

B1:

Company B does not enforce Multi-Factor Authentication (MFA) across all users. This means user accounts are only protected by passwords, which may be weak or reused. Without MFA, an attacker who gains or guesses a password can access the system without additional verification, making unauthorized access much easier. Company B also has a poor FTP server configuration. This means FTP services are

exposed to the network and can be exploited by attackers through brute-force attempts or data interception since FTP transmits credentials in plaintext.

B2:

Vulnerabilities	Impact	Risk	Likelihood
MFA is not enforced across all users	An attacker could access systems by stealing or guessing a user's password. This could lead to stolen medical records, financial data, or unauthorized changes.	The risk is high because Company B handles sensitive data that could be exposed if user accounts are compromised.	The likelihood is high because password-based attacks like phishing and brute force are widespread when MFA is not enabled.
Poor FTP server configuration (exposed services)	Poor FTP server configuration (exposed services), attackers could intercept credentials or brute-force logins to gain unauthorized access. Since FTP traffic is unencrypted, sensitive data could be stolen during transmission.	The risk is high because FTP servers often store or transfer sensitive files that attackers can steal or manipulate.	The likelihood is medium to high because FTP is a common attack target, and brute-force attempts are frequent on exposed services.

Part C:

See the Final Page Or the Attached Document

Part D:

Company A & Company B Combined Topology

Device	OSI Layer	TCP/IP Layer
Firewall	Application Layer	Application
Router	Network Layer	Internet
Servers	Application Layer	Application
Cabling	Physical Layer	Network Interface
VPN	Network Layer	Internet
Laptops & Worksation	Application Layer	Application
Switches	Network Layer	Internet
Azure	Application Layer	Application
Wireless Access Point	Data Link Layer	Network Interface
Printer / Copier	Application Layer	Application

Part E:

Items Purchased:

MikroTik CCR2004-16G-2S+ Router

The MirkoTIk CCR2004-16G-2S+ Router, sitting at a price point of $465.00, was purchased to replace the End-Of-Life Cisco 7600 router at Company A and the consumer-grade Verizon FIOS CR1000A router at Company B. This router is a very cost-effective alternative that offers almost the same capabilities as higher-end enterprise routers at a fraction of the cost.

HPE Aruba 2930F Switches

The HPE Aruba 2930F Switches were purchased primarily for Company A to replace the end-of-life routers. Each unit costs roughly $ 1,470.00. I decided to buy this device because it was significantly

cheaper than the newer Cisco router models & Company B already had this device in use, thus meaning they had familiarity with it.

FortiGate 60F Firewall

The FortiGate 60F firewall was purchased to replace the End-of-Life FortiGate 800D at Company A and the Sophos XG firewalls at Company B, which are approaching their EOL date in March 2025. With this firewall, there is also a bundle deal to acquire a one-year Unified Threat Protection from FortiGate. The cost of this bundle would be $1,398.00.

Windows 11 Pro Licenses

The upgraded Pro Licenses were needed to remove the End-Of-Life operating systems from the workstations & laptops. The cost for these licenses was about $39.35 per license. It's necessary to upgrade these systems because the operating systems are no longer supported, which means they are highly vulnerable to malware, viruses, and other attacks.

Azure Cloud Service

Azure cloud service was needed to host all on-premise server capabilities. This cloud service will replace the end-of-life Windows servers that the companies were using. The estimated cost of annual hosting is $32,236.80.

Untouched Components:

Cables

The cables had no flaws & there was no need to replace them. They can sufficiently support the new hardware & network speeds.

Wireless Access Point

The Wireless access points didn't need any change because they were not at End-of-Life & can support the required network speed.

HPE Aruba 2930F Switch

The HPE Aruba 2930F Switch didn't need to be changed because the manufacturer still supports this switch.

Part F:

The two principles I implemented for the new topology were zero trust & defense in depth. In the updated topology, there are locks along every connection between devices. These locks represent zero trust. Users will be forced to authenticate to use these devices at every connection point. Defense in depth is expressed through the shield symbols near the defense mechanisms.

Part G:

The relevant compliances for this company merger would be the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA). Company A operates in the financial industry and serves its customers with financial products, such as checking accounts, bank cards, and investment products. Since Company A may process, transmit, or store cardholder data. Company A is required to comply with the PCI DSS. Company B must also comply with the PCI DSS because it will use credit cards for its specialized software as a payment option. The updated topology removes both the EOL hardware and software. This removal ensures that the systems will be protected from possible vulnerabilities, which is mandatory to comply with PCI DSS. Company B specializes in providing software to medical providers. Any business that deals with sensitive health information must comply with HIPAA. The updated topology uses the Azure cloud for all server

capabilities. This change removed all the EOL servers, thus protecting sensitive health data. To comply with HIPAA, a company must have technical safeguards to protect Protected Health Information (PHI). Azure cloud provides multiple security controls, such as data encryption and access management, that will align with HIPAA's technical safeguard requirements.

Part H:

When two companies merge, the attack surface increases. Additional employees and systems create additional vectors for attackers to take advantage of. Social engineering is a high-risk endeavor. Attackers learn login credentials via phishing or pretexting. Using compromised accounts, they have illegitimate access to the PII of consumers. From the network security perspective, compromised accounts give attackers mechanisms for bypassing defenses. This increases the likelihood of a massive-scale data breach. From an operational perspective, the risk can include using malware or ransomware. This causes service disruption, downtime, and decreased reliability. To manage this risk, you will need to enforce mandatory security awareness training. Perform phishing simulations to gauge employee reaction. Enforce multi-factor authentication on principal systems. Require employees to report suspicious emails right away. This offers multiple levels of protection against social engineering. Another risk to consider is a supply chain attack. Such attacks occur when a trusted supplier introduces malicious code into software or firmware, which is then relayed to the customer. With the combined company installing new servers, switches, and firewalls, there is also a chance that any one of these principal pieces of equipment is infected upon delivery. From a network security perspective, an infected piece of equipment enables intruders to circumvent defenses at the firmware or hardware level. This creates persistent access that cannot be readily found. From an operational perspective, hidden malicious code may decrease network reliability, disrupt traffic, or create outages. In mitigation against this threat, you must acquire hardware and software exclusively from known sources with verified security controls. Require vendors to provide

proof of code integrity and current security audits. Implement rigorous patch management and firmware verification methodologies.

Part I :

My proposed recommendations for the newly merged network are secure & cost-effective. The recommendation includes retiring all End-of-Life assets, migrating server capabilities to the cloud & staying under the $50,000 budget whilst ensuring compliance with all regulatory requirements of the merged company.

Summary of first-year expenses

- MikroTik CCR2004-16G-2S+ Router(2 units):$930.00, replaced two unsupported routers
- HPE Aruba 2930F Switches(4 units): $5,880, replaced four outdated switches
- FortiGate 60F Firewalls (2 units):$1,398.00,replaced two firewalls
- Windows 10 Pro Licenses(29 units): $1,158.55,29 workstations
- Azure Cloud Hosting: $32,236.80, migrated all server workloads

On-Premises Infrastructure

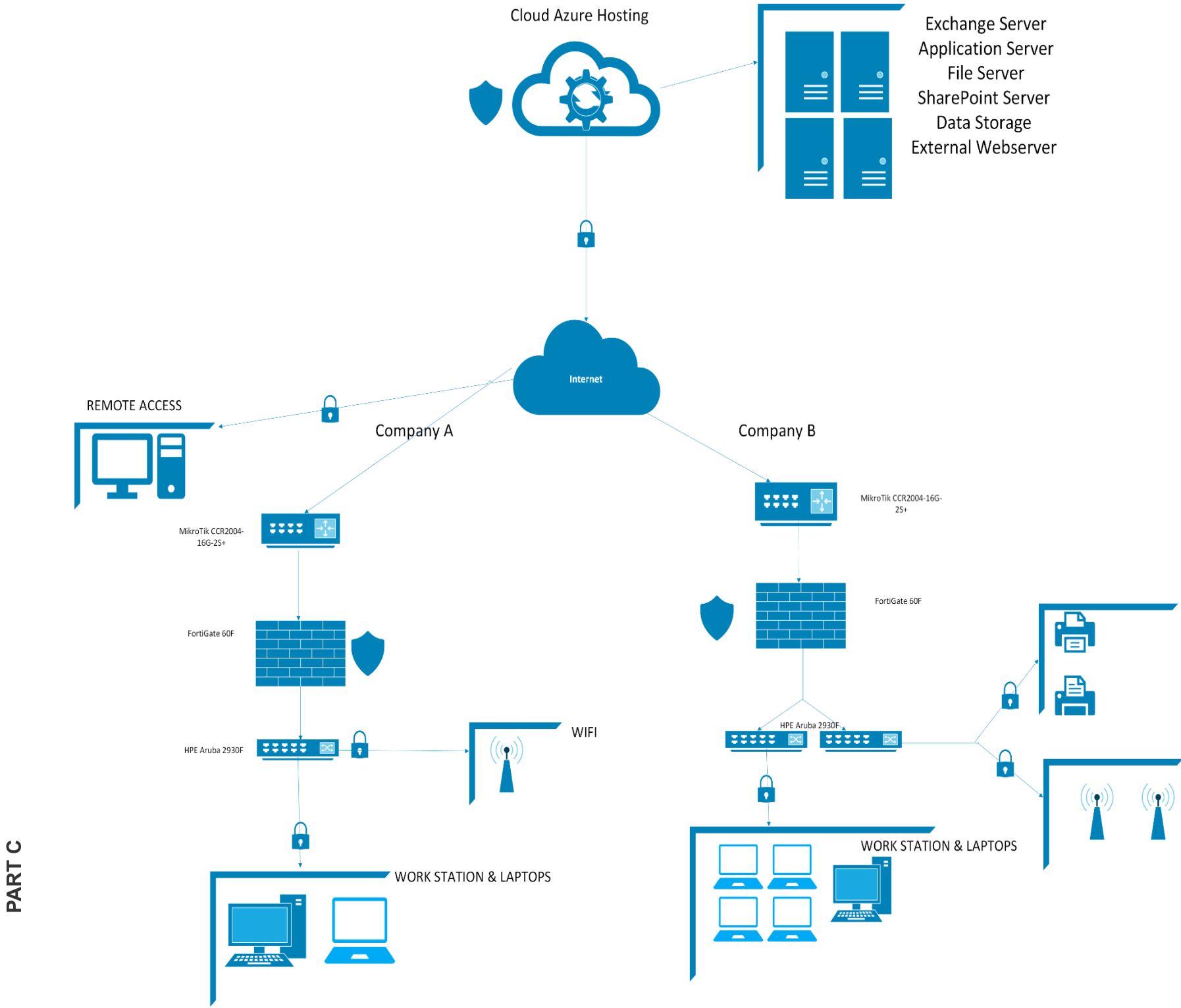
Pros	Cons
You retain complete control over your data & hardware.	You are responsible for all maintenance, management & operational costs.
You can have direct access to your data & hardware	Scaling your business up or down can be a tedious & slow task.
	It may be expensive to purchase server & networking equipment all at once

Cloud Infrastructure

Pros	Cons
The capital expenditure may be more manageable, since it’s not all up front payment	Dependent on internet connectivity.
Cloud services allow you to scale resources up or down to match your business scale	Subscription costs add up over time
Cloud services can offer a higher level of security	Data control is delegated to the cloud provider
Reduced hardware management	

Justification

The design removes all significant risks of unsupported hardware and systems. The outlined design is directly PCI DSS and HIPAA compliant. Moving workloads to Azure helps the company scale, be redundant, and reduce operational risk. The design aligns with executive goals of cloud adoption and modernization. The whole solution fits within first-year spending, and it's cost-efficient, efficient, and secure.


Cloud Azure Hosting
Exchange Server
Application Server
File Server
SharePoint Server
Data Storage
External Webserver
Internet
REMOTE ACCESS
Company A
Company B
MikroTik CCR2004-16G-2S+
MikroTik CCR2004-16G-2S+
FortiGate 60F
FortiGate 60F
HPE Aruba 2930F
HPE Aruba 2930F
WIFI
WORK STATION & LAPTOPS
WORK STATION & LAPTOPS

PART C

References

PCI Security Standards Council. (n.d.). ***PCI Security Standards Council – Protect payment data with industry-driven security standards, training, and programs.***

https://www.pcisecuritystandards.org/

Palo Alto Networks. (n.d.). ***What is PCI DSS?***

https://www.paloaltonetworks.com/cyberpedia/pci-dss

U.S. Department of Health & Human Services. (n.d.). ***OCR complaint portal assistant.***

https://ocrportal.hhs.gov/

U.S. Department of Labor. (n.d.). ***Health Insurance Portability and Accountability Act (HIPAA).*** **https://www.dol.gov/agencies/ebsa/laws-and-regulations/laws/hipaa**

MikroTik CCR2004-16G-2S+. (n.d.). ***slashdot.org.***

https://slashdot.org/software/p/Cisco-1000-Series-Aggregation-Services-Routers/alternatives

HPE JL262A Aruba 2930F 48G PoE+ 4SFP Switch NEW. (n.d.). ***serversupply.com.***

https://www.serversupply.com/NETWORKING/SWITCH/48%20PORT/HPE/JL262A_299334.htm

FortiGate-60F Hardware plus 1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP). (n.d.). ***avfirewalls.com*****.**

https://www.avfirewalls.com/fortigate-60f.asp

Microsoft Windows 10 Professional 64 -bit OEM. (n.d.). ***walmart.com*****.**

https://www.walmart.com/c/kp/windows-10-pro-retail

Microsoft. (n.d.). ***Windows Server pricing*****.**

https://www.microsoft.com/en-us/windows-server/pricing

Microsoft. (n.d.). ***Azure Windows Server licensing FAQ*****.**

https://azure.microsoft.com/en-us/pricing/licensing-faq

Microsoft. (n.d.). ***Windows Server 2012 and Windows Server 2012 R2 are at the end of support*****.**

https://learn.microsoft.com/en-us/lifecycle/announcements/windows-server-2012-r2-end-of-support

Threatscape. (n.d.). ***Windows Server 2012 is approaching end of life*****.**

https://www.threatscape.com/cyber-security-blog/windows-server-2012-is-approaching-end-of-life/

University of Alaska Anchorage. (n.d.). ***Windows XP - End of life*****.**

https://www.uaa.alaska.edu/about/administrative-services/departments/information-technology-services/getting-help/knowledge-base/windows-xp-end-of-life.cshtml

Microsoft. (n.d.). ***FAQ about the end of support for Windows 7.***

https://learn.microsoft.com/en-us/troubleshoot/windows-client/windows-7-eos-faq/windows-7-end-support-faq-general

University of California, Berkeley. (n.d.). ***Windows 7 EOL.***

https://security.berkeley.edu/topics/windows-7-eol

Park Place Technologies. (n.d.). ***Cisco 7600 series routers.***

https://www.parkplacetechnologies.com/eosl/cisco/cisco-7600-series-routers/

ReluTech. (n.d.). ***Cisco 7600 series routers.***

https://relutech.com/eol-eosl/cisco/cisco-7600-series-routers

Park Place Technologies. (n.d.). ***Catalyst End Of Life List.***

https://www.parkplacetechnologies.com/eosl/family/catalyst/

ReluTech. (n.d.). ***Cisco 3750X.***

https://relutech.com/eol-eosl/cisco/catalyst-3750x

Bevan, L. (2024, December 11). ***Sophos firewall XG series EOL and XGS migration.***

https://greymatter.com/content-hub/sophos-firewall-xg-series-eol-xgs-migration/

Fortinet. (n.d.). ***Fortinet product life cycle (Hardware).***

https://tsc.openbase.co.kr/support/solutions/articles/72000623054-2024-fortinet-product-life-cycle-hardware-

Park Place Technologies. (n.d.). ***Fortinet end of life list.***

https://www.parkplacetechnologies.com/eosl/fortinet/