

Secure Network Design

Network Meger and implementation plan

Damian Yates | D482 | April 1, 2024

# Business Requirements

## Overview

Company A, a prominent global entity in the financial sector based in the United States, has recently expanded its operations by acquiring Company B. This merger necessitates a strategic integration of systems and services to enhance operational efficiency, security, and compliance, especially as Company B caters to medical providers with specialized software and credit card processing capabilities.

### Objectives

The primary objective of this project is to design and implement a secure network that leverages both on-premises and cloud infrastructures. The design will adhere to zero trust principles to safeguard sensitive financial and medical data, support scalability, ensure redundancy, and maintain compliance with all applicable regulatory standards.

### Requirements

#### Integration and Optimization

* Evaluate and integrate or phase out overlapping technical tools and capabilities between Company A and Company B.
* Maintain critical unique services of Company B, especially those tailored for medical providers.

#### Security Design

* Implement a secure network architecture based on zero trust principles, ensuring strict access controls and verification protocols.
* Incorporate both on-premises and cloud-based solutions to optimize security, flexibility, and data availability.

#### Cloud Utilization

* Adopt cloud technologies to enhance infrastructure scalability and redundancy.
* Utilize cloud-based security services to manage identities, access controls, and data protection.

# Business Requirements (cont.)

#### Compliance and Regulatory Adherence

* Ensure full compliance with financial and medical industry standards, including but not limited to GDPR, HIPAA, and PCI-DSS.
* Establish ongoing monitoring and reporting mechanisms to adapt to regulatory changes and maintain compliance.

#### Budget and Resource Allocation

* Adhere to the allocated budget of $50,000 for the first year to cover the costs associated with the secure network design and implementation.
* Prioritize investments in critical security capabilities and cloud integration to maximize ROI and ensure long-term sustainability.

#### Professional Expertise

* Leverage the established cybersecurity team of Company A to provide comprehensive training and integration for existing IT staff from Company B, thereby assimilating them into the cybersecurity procedures and culture of Company A.
* Continue leveraging third-party support strategically for non-core infrastructure needs while maintaining oversight and compliance.

### Deliverables

* A detailed secure network design document outlining the architecture, technologies used, and implementation roadmap.
* A compliance framework document detailing the regulatory requirements and compliance strategies.
* A project timeline with key milestones and deadlines for the integration and security enhancements.

### Evaluation Metrics

* Achievement of a seamless integration with minimal disruption to existing services.
* Implementation of a fully compliant and secure network infrastructure within the allocated budget.
* Demonstrable improvement in operational efficiency and security posture post-integration.

# Identified Vulnerabilities

## Company A

### Network Security Problems:

1. Open ports 21-90, 3389: Open ports can expose the network to unauthorized access and potential exploitation. Port 21 is traditionally used for FTP, which is not secure. Similarly, port 3389 is used for Remote Desktop Protocol (RDP) access, which can be vulnerable to brute force attacks if not properly secured.
2. All users use eight-character passwords: Short, simple passwords are easier to crack with modern password-cracking tools. This practice does not adhere to strong password policies, which usually require more complex and longer passwords to increase security.

### Infrastructure Problems:

1. End-of-Life Equipment in use: Using outdated equipment that is no longer supported by the manufacturer can pose significant security risks due to the lack of security patches and updates. This can leave the infrastructure vulnerable to known exploits.
2. Cable Plant - Cat5e: While Cat5e is a capable standard, it may not support the latest speed requirements and could be susceptible to interference and crosstalk, potentially impacting network performance. Additionally, if the cabling is old or poorly maintained, it could contribute to network issues or vulnerabilities.

## Company B

### Network Security Problems:

#### Critical Vulnerabilities in Services:

* + Distributed Ruby (dRuby/DRb)Multiple Remote Code Execution Vulnerabilities (Critical Severity): This poses a high risk as it can allow attackers to execute arbitrary code remotely.
  + Java RMI ServerInsecure Default Configuration Remote Code Execution Vulnerability (Critical Severity): Exposes the server to remote code execution if left unpatched or not securely configured.

# Identified Vulnerabilities (cont.)

#### Insufficient Access Control:

* + MFA not enforced across all users (High Risk): Without Multi-Factor Authentication, the system is more vulnerable to unauthorized access.
  + All users have local administrative privileges (Moderate Risk): This practice can lead to an increased risk of accidental or deliberate misuse of privileges.

### Infrastructure Problems:

#### End-of-Life Operating Systems:

* + Operating System (OS) End of Life (EOL) Detection (Critical Risk): The use of end-of-life operating systems can expose the network to vulnerabilities that will not be patched by the manufacturer.
  + Consumer-Grade Border Router:Utilization of the Verizon FIOS router (CR1000A) as a border router presents risks due to its consumer-grade design, which may lack the necessary security features and throughput capacities for enterprise-level protection and traffic management.

#### Vulnerable Network Protocols and Services:

* + FTP Brute Force Logins Reporting (High Risk): Indicates that the FTP service is not secure, especially if it's using the standard FTP protocol, which transmits credentials in clear text.
  + Apache Tomcat AJP RCE Vulnerability (Ghostcat) (Critical Risk): If the AJP port is exposed without proper security, it can lead to a remote code execution vulnerability.

# Impact, Risk, & Likelihood

## COMPANY A

### Network Security Problems:

#### Open ports 21-90, 3389:

Impact: High - Unauthorized access could lead to data breaches and system compromise.

Risk: High - These ports are commonly targeted for exploitation.

Likelihood: High - Open ports are one of the most common attack vectors.

#### All users use eight-character passwords:

Impact: Moderate to High - If passwords are compromised, it could lead to unauthorized access.

Risk: High - Short passwords are significantly easier to crack.

Likelihood: High - Due to the prevalence of password-cracking tools.

### Infrastructure Problems:

#### End-of-Life Equipment in use:

Impact: High - Potential for unpatched vulnerabilities to be exploited.

Risk: High - Outdated equipment is known to be a major security risk.

Likelihood: Moderate to High - Depends on the existence of known exploits.

#### Cable Plant - Cat5e:

Impact: Low to Moderate - Could lead to performance degradation but not typically a direct security risk.

Risk: Moderate - Higher susceptibility to interference could impact integrity of sensitive operations.

Likelihood: Moderate - Dependent on the environmental conditions and age of the cabling.

# Impact, Risk, & Likelihood (cont.)

## COMPANY B

### Network Security Problems:

#### Critical Vulnerabilities in Services:

Impact: High - Remote code execution could lead to complete system takeover.

Risk: High - Critical vulnerabilities are attractive targets for attackers.

Likelihood: High - Publicly known critical vulnerabilities are likely to be exploited.

#### Insufficient Access Control:

Impact: High - Could lead to unauthorized access and internal breaches.

Risk: High - Lack of MFA and excessive privileges are significant security concerns.

Likelihood: Moderate to High - These weaknesses are often exploited by attackers.

### Infrastructure Problems:

#### End-of-Life Operating Systems:

Impact: High - Could lead to breaches, as EOL systems do not receive security updates.

Risk: High - Known EOL systems are often targeted by attackers.

Likelihood: High - The existence of known vulnerabilities increases the chances of exploitation.

#### Consumer-Grade Border Router:

Impact: High - A compromised router could impact the entire network.

Risk: Moderate to High - Consumer-grade devices are not designed for robust enterprise security.

Likelihood: Moderate - This depends on whether targeted attacks are likely given the company's profile.

# Impact, Risk, & Likelihood (cont.)

### Vulnerable Network Protocols and Services:

#### FTP Brute Force Logins Reporting:

Impact: Moderate - Could lead to credential compromise and data leakage.

Risk: High - FTP is an outdated and insecure protocol.

Likelihood: High - Brute force attacks are common on FTP services.

#### Apache Tomcat AJP RCE Vulnerability (Ghostcat):

Impact: High - Could result in unauthorized data access or system control.

Risk: High - This well-known vulnerability is a critical security risk.

Likelihood: Moderate - Exploitation depends on the visibility and access to the vulnerable service.

# Topology Diagram

A diagram of a network

Description automatically generated

# Topology Components

|  |  |
| --- | --- |
| Device | Cost Estimate |
| FortiGate 800D x2 | $0 – Existing Hardware |
| FortiGate 90G x2 | $2,800 |
| Aruba 7024 (JW683a) | $5,200 |
| Aruba 2930F (JL256A) x6 | x5 - $6,500 |
| Aruba 535 x 10 | $0 – Existing Hardware |
| Cat 6a UTP install | $3,800 per 2000ft |
| M365 Business Premium | $264 annual per user |
| Workstations | $0 – Existing Hardware |
| Printers | $0 – Existing Hardware |
| Servers | $0 – Existing Hardware |

### Associated Communication Layers

#### FortiGate 800D and FortiGate 90G:

* + OSI Model Layers: Firewalls typically operate at multiple layers of the OSI model, including the Network layer (Layer 3) where routing and IP addressing occur, and the Transport layer (Layer 4) where TCP/UDP ports are managed. Advanced firewalls can also inspect up to the Application layer (Layer 7).
  + TCP/IP Model Layers: Corresponds to the Internet layer and Transport layer primarily but may involve the Application layer for deep packet inspection and other advanced features.

#### Aruba 7024 (JW683A):

* + OSI Model Layers: Mobility controllers are used to manage wireless network traffic and configurations, generally functioning from Layer 2 (Data Link) to Layer 7 (Application), depending on the specifics of traffic management and network services provided.
  + TCP/IP Model Layers: This device operates from the Network Access layer up to the Application layer, managing network traffic and configuration for wireless devices.

##### Aruba 2930F (JL256A):

* + OSI Model Layers: Primarily operates at Layer 2 (Data Link) but can have Layer 3 (Network) capabilities if configured for routing functions.
  + TCP/IP Model Layers: Primarily the Network Access layer, with potential functionality at the Internet layer if routing is enabled.

# Topology Components (cont.)

##### Aruba 535:

* + OSI Model Layers: Wireless access point that mainly operates at Layer 2 (Data Link) but also involves Layer 1 (Physical) due to the nature of wireless transmission and can extend to Layer 3 (Network) for IP addressing and routing.
  + TCP/IP Model Layers: Mainly the Network Access layer, with some influence on the Internet layer for network communications.

##### Cat 6a UTP install:

* + OSI Model Layers: Category 6a cabling is physical infrastructure and thus pertains solely to Layer 1 (Physical) of the OSI model.
  + TCP/IP Model Layers: This relates to the Network Interface layer, providing the physical means for data transmission.

##### M365 Business Premium:

* + OSI Model Layers: As a suite of office productivity software delivered over the internet, it primarily operates at Layer 7 (Application).
  + TCP/IP Model Layers: Functions at the Application layer, where software applications communicate over the network using internet protocols.

# Rationale

This proposed architecture places a strong emphasis on identity as the new security perimeter, with Microsoft Cloud Services serving as the cornerstone for ensuring that only authenticated and authorized users and devices can access resources, efficient threat detection and alerting and managing information protection and compliance adherence. It assumes all traffic is untrusted until vetted, ensuring comprehensive security from the user endpoint to the cloud. The Aruba wireless controller recommended should be chosen based on the current and projected future needs of the merged organization in terms of client density, throughput, and specific features required for compliance and security.

# Secure Network Principles

Zero-Trust Architecture: Employ the principle of least privilege in the zero-trust model by continuously authenticating and verifying every device and user before access to network resources is granted. Implement Microsoft Entra and Intune, alongside Conditional and Role-Based Access controls, to manage identities, device access, and permissions effectively. This ensures that users and systems are only granted access to the resources necessary for their roles, in alignment with the segregation of duties and economy of mechanism principles. (Peterson, 2023)

Firewall and Routing: Transition from Cisco and Verizon routers to clustered FortiGate 800D and 90G solutions for both intra-VLAN routing and perimeter defense at each office. This change centralizes routing, firewall policies, and security inspections within the FortiGate devices, supporting a defense in depth strategy by layering security measures. (Matthews, 2022)

Wireless Network Management: Implement an Aruba 7000 Series Mobility Controller to manage a network of Aruba APs. This setup centralizes the management and enforces access control policies that are sensitive to user identity, device type, location, and other contextual factors, following the principles of least privilege and fail-safe defaults.

Identity and Access Management with Microsoft Entra: Utilize Microsoft Entra for comprehensive access and identity management across the organization. Dynamic permission granting based on the security posture of each access request enforces conditional and role-based access policies, supporting segregation of duties and least privilege access controls.

Server Infrastructure and Security: Migrate all virtual servers to Azure, securing them through Microsoft Entra. This cloud-based environment is configured to strictly enforce least privilege access controls and multi-factor authentication, exemplifying economy of mechanism and fail-safe defaults.

Wireless Authentication: Leverage the built-in capabilities of the Aruba wireless controller to authenticate wireless connections, integrating with Microsoft Entra to ensure identity-based access controls. This aligns with zero trust principles by verifying and authorizing each connection based on comprehensive security assessments.

# Secure Network Principles (cont.)

Compliance Facilitation with Microsoft Purview and Defender: Use Microsoft Purview for compliance with SOX, PCI, and GDPR by classifying, labeling, and protecting sensitive information across the organization. Automate compliance checks and report generation for audits, and implement data protection policies to control and monitor access to sensitive data. Logging and retention policies ensure data is kept in a secure, immutable format, crucial for SOX compliance and adhering to the principle of fail-safe defaults.

Data Residency and Sovereignty: For GDPR compliance, configure Azure services to comply with data residency and sovereignty rules, ensuring data is stored and processed in appropriate geographical locations, which supports the principle of fail-safe defaults.

PCI Compliance: Isolate cardholder data environments within the network to ensure they adhere to PCI compliance standards. Use Defender’s threat detection and response capabilities to protect against breaches and maintain a detailed audit trail, aligning with defense in depth and segregation of duties principles.

# Regulatory Compliance

The proposed merged network topology addresses several regulatory compliance requirements. Two key compliance requirements relevant to financial and healthcare entities are the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR).

### PCI DSS Compliance

* Relevance: PCI DSS applies to all organizations that handle credit card information, ensuring that this sensitive data is kept secure from breaches and fraud. For the newly merged company, especially with Company B's acceptance of credit card payments, adherence to PCI DSS is crucial to protect customer data and maintain trust.
* How It’s Addressed: The merged network topology includes clustered FortiGate 800D firewalls for robust security and network segmentation. This design can create a Cardholder Data Environment (CDE) that is separate from the rest of the network, limiting access to cardholder data as per PCI DSS requirements. (Kumar, 2022) Additionally, the use of Microsoft Defender for threat detection and response can help in monitoring and protecting the CDE against breaches, another key PCI DSS requirement.

# Regulatory Compliance (cont.)

### GDPR Compliance

* Relevance: GDPR imposes strict rules on data privacy and the handling of personal data for entities operating in the EU or dealing with EU citizens' data. The merged company must ensure the protection and proper handling of personal information, requiring stringent data security measures and policies.
* How It’s Addressed: The topology leverages Microsoft Cloud Services, including Azure and Microsoft Entra, which provide tools for data classification, loss prevention, and access controls, all of which are fundamental for GDPR compliance. The zero-trust model inherent in the design, where identity verification is central, aligns with GDPR's principles of least privilege and access necessity. The network's security measures, facilitated by a centralized Aruba wireless controller and advanced firewalls, can prevent unauthorized access to personal data and provide the required data processing transparency and reporting capabilities mandated by GDPR. (Richardson, 2024)

This architecture ensures that only authenticated and authorized users and systems can access the resources for which they have permissions, significantly reducing the risk of data breaches. Moreover, the infrastructure can produce audits and logs that support GDPR's accountability and reporting requirements.

# Emerging Threats

Emerging threats in cyberspace are continually evolving, posing new challenges for organizational security postures. For a merged organization with a complex network topology, two such threats could be the rise of sophisticated phishing attacks targeting cloud-based services and the potential exploitation of zero-day vulnerabilities in network devices and software.

### Advanced Phishing Attacks on Cloud Services

* Security Risks: As organizations move to cloud-based platforms like Azure, attackers are crafting more sophisticated phishing campaigns to gain access to cloud services. This can lead to unauthorized access to sensitive data and systems. An attacker might, for instance, spoof a login page for Microsoft Entra or Azure services to capture user credentials.
* Performance Impacts: An indirect impact of such attacks can be an increase in the load on network resources due to unauthorized access attempts, potentially leading to performance degradation.

# Emerging Threats (cont.)

* Management of Risks: To manage these risks, the organization should implement robust multi-factor authentication (MFA) across all cloud services and provide extensive user training on identifying phishing attempts. Regular security awareness programs should be conducted to educate employees about the latest phishing tactics. In addition, the use of advanced threat protection solutions in Microsoft Defender can help identify and block phishing attempts and abnormal sign-in activities.

### Zero-Day Exploits in Network Infrastructure

* Security Risks: Zero-day exploits, which are previously unknown vulnerabilities, can be particularly problematic for merged organizations that may have a large and complex network topology with various devices and software. These vulnerabilities could be exploited before vendors release patches, potentially giving attackers deep access to network resources.
* Performance Impacts: The exploitation of zero-day vulnerabilities could lead to unauthorized resource consumption, network scanning, or spreading of malware within the network, resulting in network slowdowns or outages.
* Management of Risks: To mitigate these risks, the organization should adopt a proactive approach to security, which includes subscribing to threat intelligence services for early warning of such exploits. Regularly updating and patching all network devices and software is crucial. Implementing intrusion detection and prevention systems (IDS/IPS) can help identify unusual network patterns that might indicate an exploitation attempt. In addition, deploying web application firewalls (WAFs) and regular penetration testing can be instrumental in identifying and mitigating potential zero-day exploits. Network segmentation can limit the spread of an attack if a zero-day exploit occurs.

In both cases, it's important for the merged organization to invest in advanced security monitoring and incident response capabilities. By actively monitoring network traffic and using automated response solutions, the organization can quickly respond to and mitigate the effects of emerging threats.

# Summary Recommendations

### Cost-Benefit Analysis for On-Premises and Cloud Infrastructure Solutions:

* On-Premises: On-premises solutions typically involve higher initial capital expenses for hardware, software, and the physical space to house the infrastructure. The organization will also incur ongoing expenses for maintenance, power, cooling, and personnel. However, on-premises infrastructure offers full control over the hardware, which can be essential for certain regulatory requirements, and may provide lower latency for internal applications.
* Cloud Infrastructure: Cloud solutions, like Azure, shift much of the capital expenses to operational expenses, with a pay-as-you-go model. This reduces the upfront costs and offloads maintenance to the cloud provider. Cloud services offer scalability and flexibility, enabling the organization to adjust resources according to demand. Although there is a recurring cost, the company benefits from the latest technology, built-in resilience, and robust security measures that cloud providers maintain. (O'Donnell, 2023)

Considering the merger, the combined entity likely has fluctuating and growing needs, making the scalability of cloud infrastructure highly advantageous. The upfront savings, coupled with the cloud's advanced security features like those provided by Microsoft Entra and Defender, present a compelling case for migrating to a cloud-centric model.

### Justification for Implementation Recommendations:

* Security: The zero trust model is vital in today’s threat landscape. Leveraging identity verification and access management through Microsoft Entra aligns with this principle and ensures that only verified users and devices can access the network, reducing the risk of data breaches.
* Compliance: For a company operating with financial and medical data, compliance with regulations like SOX, PCI, and GDPR is non-negotiable. Cloud providers offer tools that aid in compliance, and their constant updates can help the company stay compliant with evolving regulations.
* Performance and Reliability: The proposed Aruba wireless solution with a high-performance controller caters to the current and future wireless demand, ensures high availability, and supports the authentication needs of the organization. The clustered FortiGate 800D setup is aligned with the need for fault tolerance and high availability for critical network functions.

# Summary Recommendations (cont.)

* Cost Savings and Efficiency: Cloud infrastructure can potentially offer cost savings over time, especially when considering the efficiency gains from reduced downtime and the ability to rapidly deploy new services. Moreover, the pay-as-you-go model aligns well with the variable nature of a newly merged company's demands.
* Future Scalability: As the company grows, the need for additional resources will increase. The cloud's scalability ensures that the organization can expand its infrastructure swiftly without the delay of procuring and setting up physical hardware.

Overall, the recommendations for a secure merged network design balance the need for advanced security, regulatory compliance, performance, cost efficiency, and scalability to support the organization's operations and strategic objectives.