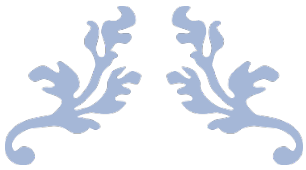


SECURE NETWORK DESIGN

Jamal Rizki

Table of Contents

Current Network and Infrastructure Problems

Two current network security problems found at Company A are:

1. Weak Passwords – The risk analysis uncovered the use of weak passwords. Using 8-character passwords opens up the risk of attack by bad actors.
2. Out-of-Date Operating systems – It was found that several workstations are still running deprecated operating systems.

Two current Infrastructure problems found at Company A are:

1. End-of-life Equipment – It was found that end-of-life equipment is being utilized.
2. Open ports – Several open ports were found to be left open across the network.

Two current network security problems found at Company B are:

1. No enforcement of multi-factor authentication – It was uncovered that the use of MFA is not currently being implemented.
2. At present, all users have local administrative privileges – The vulnerability report showed local administrative privileges on the network.

Two current Infrastructure problems found at Company B are:

1. End-of-life Equipment – The risk analysis highlighted the use of EOL and non-enterprise grade equipment in use.
2. PostgreSQL Misconfiguration – Settings in the PostgreSQL database are misconfigured with weak passwords while also being publicly accessible.

Analysis of Vulnerabilities found

Company A:

1. Weak Passwords – Currently, 8-character passwords are in use. These are generally considered weak, as they can be cracked by bad actors quite easily — especially if they lack complexity, such as special characters, numbers, and mixed case. Threat actors may also use brute-force or dictionary attacks to guess passwords and passphrases, alternatively, they may leverage leaked password lists to gain unauthorized access to accounts and systems.
2. Open Ports – Ports 21–90 and port 3389 remain unnecessarily open. This creates potential attack vectors that can be easily discovered using scanning tools. If the services behind these ports are misconfigured or have known vulnerabilities, bad actors may exploit them to gain unauthorized access to the network or systems. Leaving unnecessary ports open increases the organization's attack surface, making it easier for unauthorized users to gain access, execute malware, or escalate privileges.

Vulnerability	Impact	Risk Level	Likelihood
All users use eight-character passwords	Potential breach of employee, administrative, or executive accounts and systems	High	High
Open Ports 21-90, 3389	Unauthorized network access, malware or ransomware execution	High	High

Risk and Likelihood:

1. Weak Passwords – The use of weak, eight-character passwords presents a high-risk attack vector, as it enables well-known and widely used attacks on user credentials, such as brute-force and dictionary attacks. The likelihood of exploitation is high, as password-based attacks remain among the most common and effective techniques used by threat actors.
2. Open Ports – Leaving ports open carries a high risk, as it allows bad actors to target, interact with, and penetrate the network through these open ports. The likelihood is high, as open ports can be easily discovered using basic and widely available automated scanning tools.

Company B:

1. No Multi-Factor Authentication enforcement – Access to systems is currently only utilizing single-factor authentication. This is not considered best practice, as an attacker only needs to compromise a password to gain access to the system. MFA is a great example of the Defense in Depth principle used in cybersecurity. Multi-Factor Authentication can reduce the risk of a single point of failure by adding additional layers of protection, such as verification codes or biometrics.
2. Non enterprise grade equipment – The use of a Verizon FIOS router (CR1000A) as a border router is the current setup for the company. Using this is not advised, as the router is purposed for residential use as opposed to small business or enterprise environments. The CR1000A lacks the performance, security, and scalability needed in an enterprise environment and is not aligned with a robust implementation of core cybersecurity principles such as defense in depth.

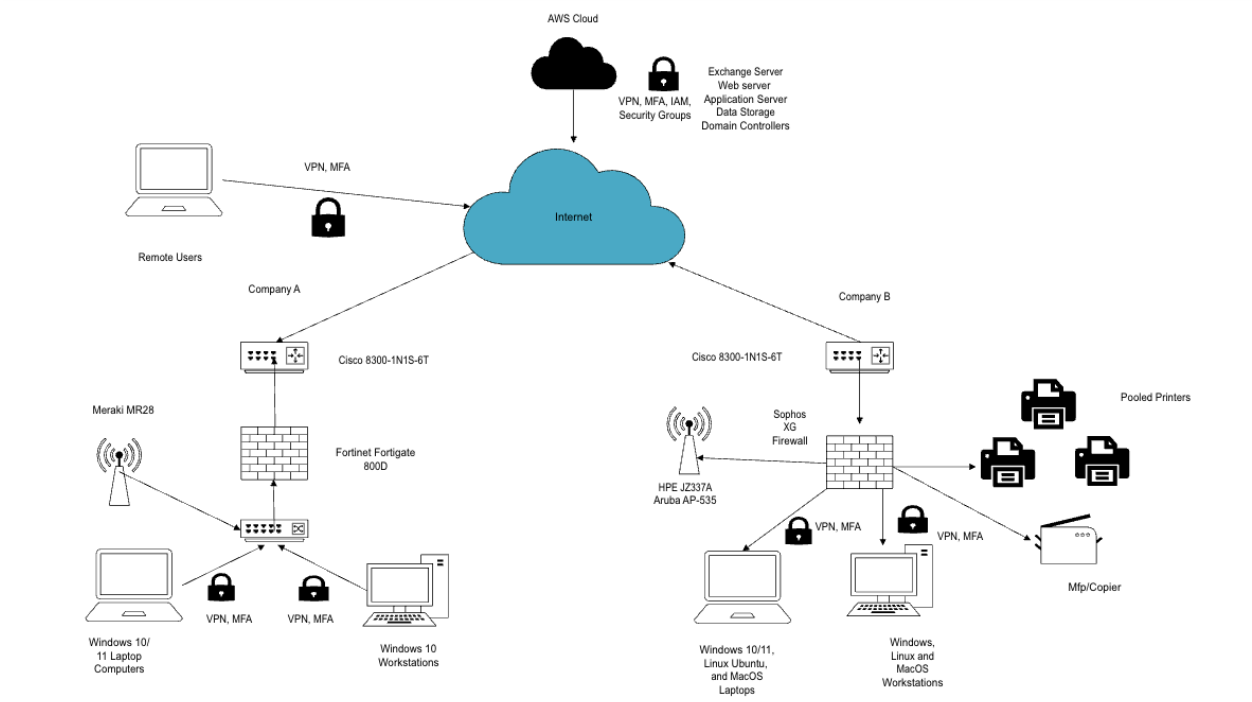
Vulnerability	Impact	Risk Level	Likelihood
MFA not enforced across all users	Full access to systems/network	High	High

	with the breach of a single password		
Non-Enterprise equipment currently used	Lack of proper network security controls increasing the risk of unauthorized access.	High	Moderate-High

Risk and Likelihood:

1. No Multi-Factor Authentication enforcement – Not enforcing multi-factor authentication carries a high risk, as it allows an attack to succeed with only a single compromised credential. The likelihood is also high, as phishing attacks and password reuse are both commonly used by threat actors and are highly effective.
2. Non enterprise grade equipment – The Verizon FIOS (CRR1000A) poses a high risk due to its lack of enterprise-grade security features necessary for a business environment. The likelihood is moderate to high, as residential equipment typically lacks essential network segmentation capabilities and security controls. This is especially critical in a business setting, and since this device also functions as a border router, the associated risks are even greater.

Network Topology Diagram of Proposed Merger



OSI and TCP Layers

Device	OSI Layer	TCP/IP Layer
Firewall - NGFW	Application – 7	Application
Router	Network – 3	Internet
Servers	Application – 7	Application
Cabling	Physical – 1	Physical
VPN	Network – 3	Internet
Laptops and Workstations	Application – 7	Application
WAP	Data – 2	Network
Printers	Application – 7	Application
Cloud Solution	Application – 7	Application
Switch	Data – 2	Network

Rationale for Upgrading, Adding, or Repurposing Network Components

Cloud Solution – The main investment in this merger is the cloud solution. It is here that we will move the web servers, application servers, Exchange servers, data storage, and domain controllers. Cloud solutions provide managed, scalable infrastructure and security controls. For this merger we will utilize Amazon Web Services, use its built-in security groups to manage access, segment the environment using a VPC, enforce multi-factor authentication, store data in S3 buckets, establish a site-to-site VPN connection as well as an AWS Client VPN, deploy AWS Managed Microsoft AD and Amazon FSx for Windows File Server, and host servers on EC2 instances. The estimated cost of this solution is $2,500–$2,700 per month or $30,000–$32,400 per year (Amazon Web Services, n.d.). More information on pricing can be found here: https://calculator.aws/

Border Routers – In both networks, the border routers are not of suitable quality: the Verizon FIOS (CR1000A) in Company B and the Cisco 7600 in Company A. These routers sit at the edge of the network, and poor infrastructure can leave the entire network exposed and vulnerable. For this merger, we will retire these devices and replace them with Cisco Catalyst C8300-1N1S-6T routers at both sites. The estimated cost of this solution is $2,999 per item or $5,998 for both networks (Network Genetics, n.d.). More information on pricing can be found here: https://www.networkgenetics.net/new-cisco-c8300-1n1s-6t-catalyst-router/

Operating Systems – Keeping operating systems up to date is essential in creating secure systems. Currently there are 14 laptops at Company A that need to be updated. As there is no longer a free upgrade option available, there will need to be new licenses purchased. The current pricing per computer is $199, so the cost of the upgrade will be $2,786 (Microsoft, n.d.). There are also multiple instances of Windows 7 being used at Company B; these devices will need to be upgraded at a later date once the exact number of machines requiring updates is determined. More information on pricing can be found here: https://www.microsoft.com/en-us/windows/business/windows-10-pro

Secure Network Design Principles Utilized

Defense in depth – In Chapter 9 of *The Security Risk Assessment Handbook*, Douglas Landoll mentions several commonly used and important cybersecurity principles. Defense-in-depth is a strategy that involves using layered security controls to strengthen and protect systems against various threats. These can include logical, physical, administrative, and technical controls—both hardware and software. For this merger, the defense-in-depth layers include firewalls to filter and inspect inbound and outbound traffic, VPNs to encrypt data in transit, MFA to mitigate the risk of account compromise, and cloud solutions that leverage IAM policies and security groups.

Zero Trust – In Chapter 7 of *The Security Risk Assessment Handbook*, Landoll also introduces the concept of Zero Trust. This is the idea that elements in a network should treat all others as untrusted outsiders. At its core, it means entities should never be implicitly trusted; they should instead go through a verification process to be granted access. There are many ways to implement Zero Trust principles into networks. Uses of the Zero Trust principle in this network merger are multifactor authentication and monitoring of network traffic across the network. It is also implemented in the cloud solution via security groups and identity management.

Regulatory Compliance Requirements

PCI DSS – PCI DSS (Payment Card Industry Data Security Standard) is a set of requirements mandated by major credit card brands such as Mastercard, Visa and American Express. The purpose of these requirements is to ensure that the storing, processing, and transmission of consumer data is done in a secure way. It also aims to reduce the risk of data breaches and instances of fraud. Not complying with these requirements can lead to fines or the loss of the ability to accept vendor credit card payments. In this instance, both companies handle and process financial data and/or credit card payments. Therefore, to meet these regulatory requirements, the proposed network will implement enhanced network security by updating an EOL firewall and moving data to a secure and segmented cloud environment. It is also in the cloud that data will be encrypted at rest, and security principles like zero trust and least privilege will be implemented to secure access to data.

GDPR – (General Data Protection Regulation) In of *Important Governance: GDPR* [Video]. Elliot, J. informs us that data protection regulation implemented and regulated by the European Union. This regulation sets forth requirements for the collection, storage, and processing of data. These regulations apply to any company in any country that deals with a European citizens data. GDPR regulation allows EU citizens to exercise certain rights regarding their data and its use, this includes, the right to access, edit, erase, and restrict data and its processing. As the proposed merger involves a global audience, meeting GDPR requirements is essential. To meet these regulations, the proposed network design will move sensitive data to the cloud where it will encrypt data in transit and at rest. Access to this data is strictly controlled using Zero Trust principles and least-privilege access. The monitoring and logging of access will be provided by the Cisco firewall. A cookie policy will be added to the consumer-facing applications.

Applicable Emerging Threats

Social Engineering – Social engineering is the art of manipulating people into making security errors, allowing threat actors to gain access to systems or give away sensitive information. Common tactics include phishing emails, installing dangerous software, and pretexting phone calls. Potential impacts can include the installation of malware causing infected systems, attackers gaining unauthorized access to systems, and the loss of sensitive data. To combat and manage these risks in the future, it is advised to commit to ongoing security awareness training to all employees, clear policies, and promoting a security-first office culture.

Supply chain attacks – Supply chain attacks involve the compromise of vendors or third-party suppliers. In these attacks, malicious code or devices are tampered with without the supplier's knowledge and inserted before they reach the target organization. Potential impacts include the insertion of ransomware, data breaches, or malware infections. To counter these threats, the organization should rigorously vet suppliers, secure network infrastructure, and monitor for unusual behavior.

Summary

In merging these networks, the total estimated cost for the first year comes to $43,684. These costs include the $32,400 allotment for the Amazon Web Services cloud solution, which moves our web, application, and Exchange servers to the cloud. The database will also be segmented in the cloud, and only those with access will have permissions to alter the data. It is also recommended to replace the current border routers with newer, more secure routers; the cost of adding two Cisco Catalyst C8300-1N1S-6T units comes to a combined $5,998. It is essential to have updated operating systems, as outdated operating systems are a widely used attack vector; the estimated cost to do this is $2,786. The remaining budget of around $8,816 will be allocated for the implementation of enterprise password management solution to address weak password vulnerabilities across both companies ($1,000), staff security awareness training

specifically focused on merger-related risks ($1,500), and the remainder has been factored in to allow for the upgrading of operating systems not yet applied or accounted for here. Once the inventory of Company B's systems has been updated, the remaining funds will be utilized. For this merger, we have moved much of our infrastructure to the cloud. Migrating the infrastructure allows for rapid scaling and provides modern infrastructure for Company B's systems. This migration also eliminates major security gaps that currently exist, such as outdated operating systems, end-of-life equipment, and the lack of multi-factor authentication. This topology also aligns with regulatory compliance requirements such as PCI DSS and GDPR. In completing this merger, we will be implementing the security design principles of defense-in-depth, network segmentation, Zero Trust, and the principal of least-privilege. The dangers of not making these updates greatly outweigh the allotted budget; the costs of breaching regulations, the negative publicity from a data breach, and the financial loss from a ransomware attack cannot be overlooked. Lastly, password policies will be implemented, open ports will be closed, privileges will be re-evaluated and assigned appropriately, and end-user training will be conducted to increase security awareness.

Works Cited

Landoll, D. J. (2021). *The Security Risk Assessment Handbook*. CRC Press. https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2759769&site=eds-live&scope=site&authtype=sso&custid=ns017578&ebv=EB&ppid=pp_61

Elliot, J. (2022, Feb 23). *Important Governance: GDPR* [Video]. PluralSight. https://app.pluralsight.com/library/courses/information-governance-gdpr/table-of-contents

Amazon Web Services. (n.d.). *AWS Pricing Calculator*. Retrieved April 20, 2025, from https://calculator.aws/

Network Genetics. (n.d.). *New Cisco C8300-1N1S-6T Catalyst router*. Retrieved April 20, 2025, from https://www.networkgenetics.net/new-cisco-c8300-1n1s-6t-catalyst-router

Microsoft. (n.d.). *Windows 10 Pro for Business*. Retrieved April 20, 2025, from https://www.microsoft.com/en-us/windows/business/windows-10-pro