D482

Secure Network Design

BY: Christobel Nweke

DATE: June 17, 2024

Network Merger and Implementation Plan

Introduction

You are the cybersecurity professional for Company A and are responsible for protecting the information of the company. Your roles include managing the company's cybersecurity capabilities and tools, conducting vulnerability management, and assessing risk to sensitive information. Company A has recently purchased Company B and wants to merge both networks.

Executives of Company A have tasked you with making risk-based decisions on integrating Company B's network with Company A's existing network. Company B has provided its latest vulnerability scans, network diagrams, and existing cybersecurity capabilities and tools. As a deliverable to the executives, you will submit your recommendations for a secure network design that merges the two networks and allows remote access for employees of both companies in the form of a merger and implementation plan.

For this project, you will use the given scenario and the following supporting documents to complete your network merger and implementation plan:

- "Company A Network Diagram",
- "Company A Risk Analysis",
- "Company B Network Diagram",
- "Company B Vulnerability Report and Cybersecurity Tools"

Scenario

Company A is a global company based in the United States that operates in the financial industry. Company A serves its customers with financial products, such as checking accounts, bank cards, and investment products. Company A has recently acquired Company B and needs to integrate with or remove similar capabilities and tools from Company B. Company B is smaller in size, has no dedicated cybersecurity professional role, and utilizes third-party support for infrastructure needs. Company B offers specialized software to medical providers and accepts credit cards as a payment option.

The executives of the newly merged company have expressed interest in integrating the use of the cloud to allow for scalability and redundancy. As the security professional of the merged networks, you are tasked with creating a secure network design that includes the use of zero trust principles and that utilizes both on-premises and cloud infrastructure. You also have been tasked with ensuring compliance with all regulatory requirements of the merged company, along with utilizing cloud-based technologies to provide security capabilities. Company executives have provided a budget of $50,000 in the first year to create a secure network design to utilize cloud-based services.

Company A Network Diagram

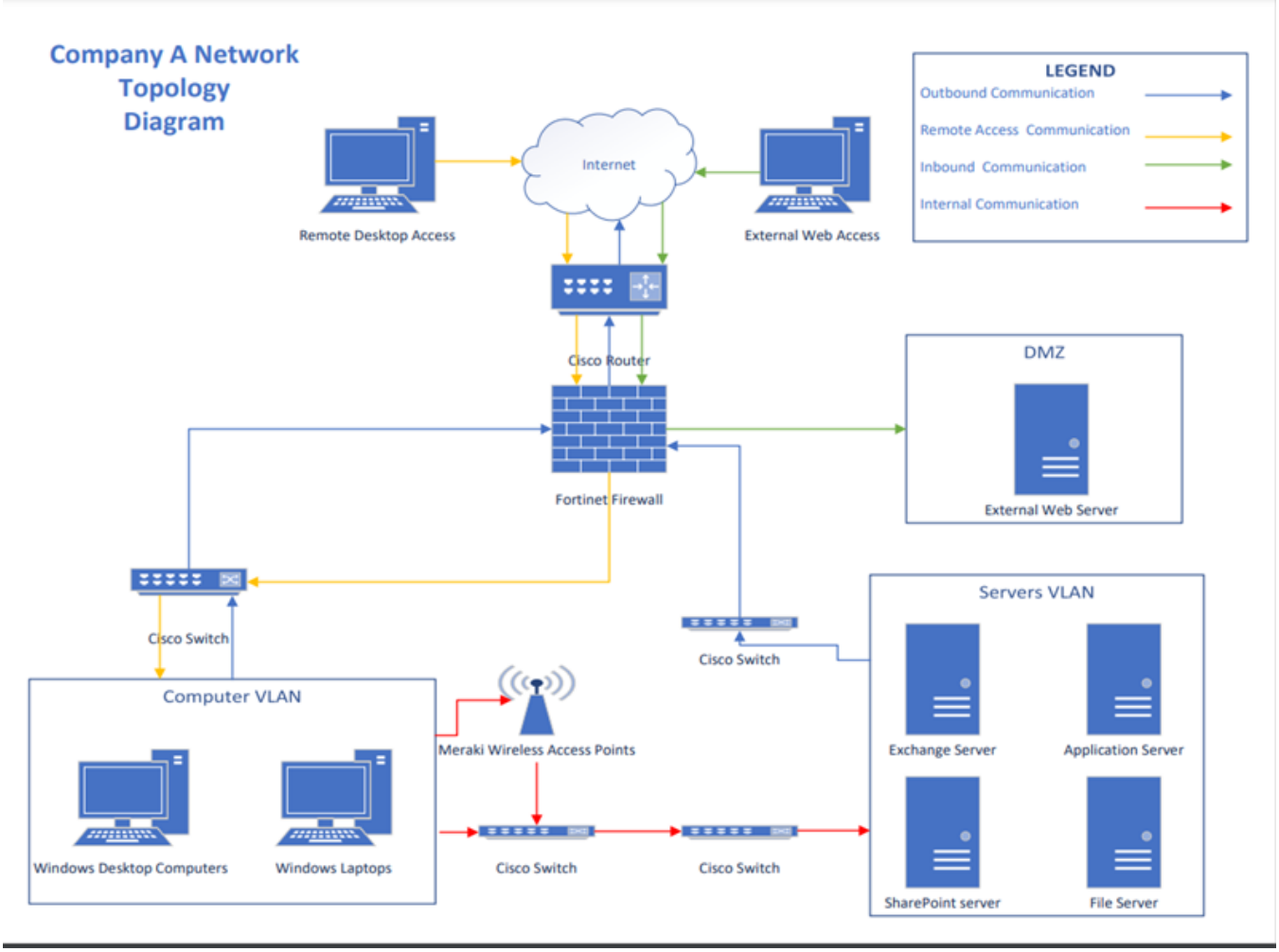

Figure 1: Company A Network Diagram

Company B Network Diagram

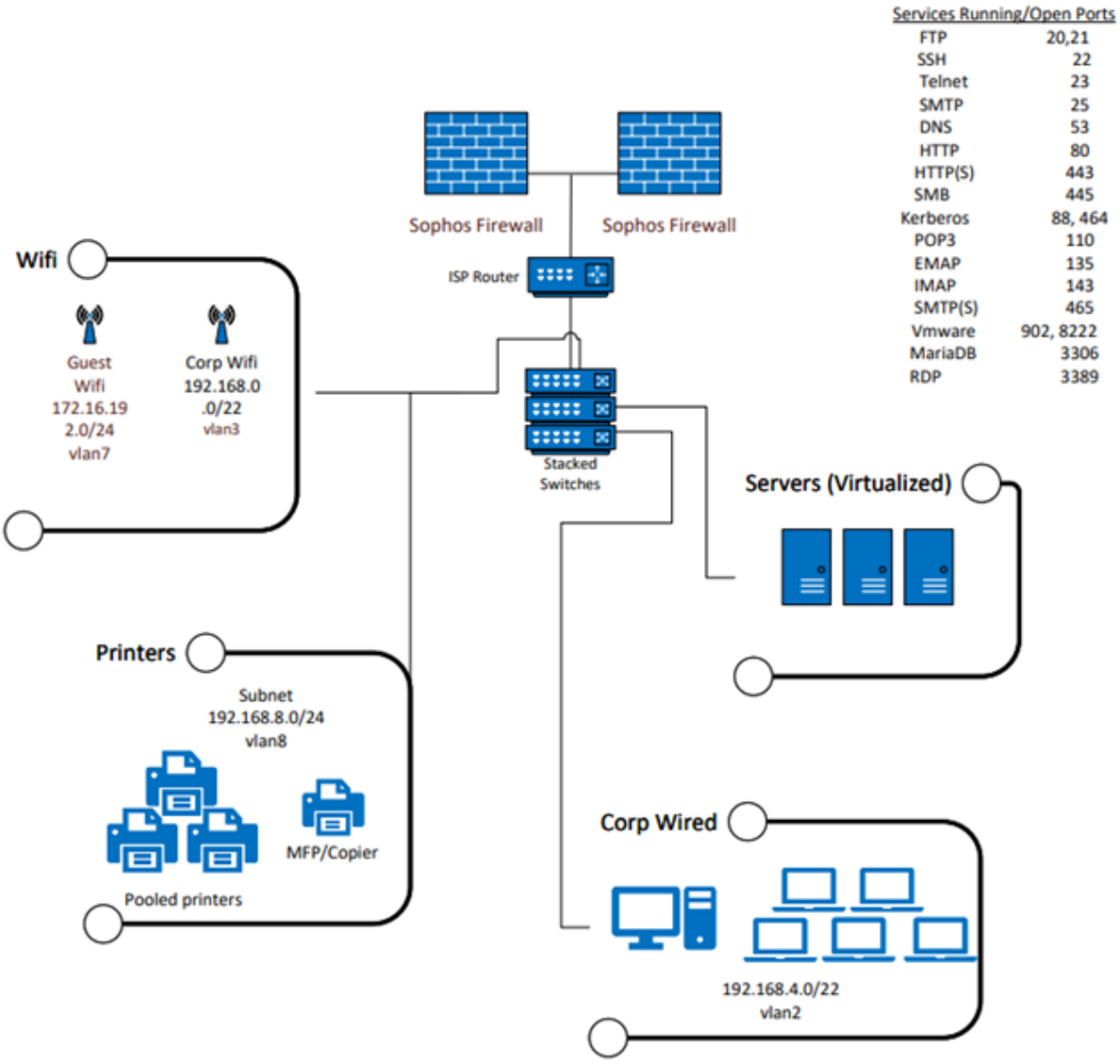

Figure 2: Company B Network Diagram

Company B Vulnerability Report

Company B performed this vulnerability assessment in anticipation of system integration with Company A. This assessment was performed by a qualified third-party assessor, and this report has been generated with the results. This assessment was performed in accordance with a methodology described in NIST 800-30 Rev 1 to identify the following:

- Vulnerabilities using the CVSS model
- Severity
- Likelihood of occurrence

Table A. Risk Classifications

Risk Level	Description
High	The loss of confidentiality, integrity, or availability may be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The loss of confidentiality, integrity, or availability may be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Low	The loss of confidentiality, integrity, or availability may be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Table B. Severity

Severity Level (CVSS Model)	**Description**
Critical	• Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices. • Exploitation is usually straightforward in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims and does not need to persuade a target user, for example, via social engineering, to perform any special functions.
High	• The vulnerability is difficult to exploit. • Exploitation could result in elevated privileges. • Exploitation could result in significant data loss or downtime.
Medium	• Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. • Denial of service vulnerabilities that are difficult to set up. • Exploits that require an attacker to reside on the same local network as the victim. • Vulnerabilities where exploitation provides only very limited access. • Vulnerabilities that require user privileges for successful exploitation.
Low	Exploitation of such vulnerabilities usually requires local or physical system access and would have little impact on the organization.

Table C. Level of Effort

Level of Effort	**Description**
High	This requires a high level of dedicated effort from one or more teams on critical systems, including patching, multiple configuration changes, or highly technical changes that risk bringing services down.
Moderate	This is a medium-level effort that requires substantial dedication from a partial or entire team. This could impact services or cause a partial outage.
Low	These are individual or small team efforts generally requiring a minimal time commitment and require running an update or remedial command or series of commands that will not impact production services.

Table D. System Inventory

System Components	
Servers	Virtualized farm running on Hyper-V (2 hosts). Windows Server 2019 and Ubuntu Linux. Approximately 20 virtualized servers (across the 2 hosts), including the following roles: • (Ubuntu Linux) FTP server for EDI Incoming Operations • 3x Domain Controllers (1 used for M365 identity sync) • 1x File Storage/Server • 1x Ruby On Rails server • 3x ElasticSearch servers (cluster) • 5x web application servers (Ubuntu Linux cluster, 1x PostGRESQL, 1x MariaDB SQL, 3x running nginX Plus w\reverse caching proxy, 1x running Apache Tomcat, PHP 8, hosting SSL/TLS certificates) • 4x Remote Desktop Servers for internal shared/applications • 2x legacy Exchange servers (post-migration)
75 Workstations	Windows XP, 7, 10/11 Pro, Ubuntu Linux, MacOS
Switches	HPE JL262A Aruba 2930F 48G PoE+
Firewall	2x Sophos XG firewalls
Border router	Verizon FIOS router (CR1000A)
Laptops	Windows 10, 11, Ubuntu 22.04 LTS, MacOS (Ventura, Monterey, Big Sur)
Wireless Access Points	10x HPE JZ337A Aruba AP-535
Cable plant	Cat6a

Table E. Risk Identification

Risk #	Vulnerability (NVT Name)	NVT OID	Severity	Risk	Level of Effort
1	Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	1.3.6.1.4.1.25623.1.0.108010	Critical	High	High
2	MFA not enforced across all users		High	High	High
3	Rexec service is running	1.3.6.1.4.1.25623.1.0.100111	High	High	Low
4	All users have local administrative privileges		Medium	Moderate	High
5	Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability on publicly-facing server	1.3.6.1.4.1.25623.1.0.140051	Critical	High	Moderate
6	Operating System (OS) End of Life (EOL) Detection	1.3.6.1.4.1.25623.1.0.103674	Critical	High	Low
7	rlogin Passwordless Login	1.3.6.1.4.1.25623.1.0.113766	High	Moderate	Low
8	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	1.3.6.1.4.1.25623.1.0.143545	Critical	High	Moderate
9	PostgreSQL weak password	1.3.6.1.4.1.25623.1.0.103552	High	High	Low
7.52	PostgreSQL admin is reachable from internet		Critical	High	Low
11	VNC Brute Force Login	1.3.6.1.4.1.25623.1.0.106056	High	High	Low
12	FTP Brute Force Logins Reporting	1.3.6.1.4.1.25623.1.0.108718	High	High	Low
13	phpinfo() output Reporting	1.3.6.1.4.1.25623.1.0.11229	High	Moderate	Low
14	vsftpd Compromised Source Packages Backdoor Vulnerability	1.3.6.1.4.1.25623.1.0.103185	High	High	Moderate
15	rsh Unencrypted Cleartext Login	1.3.6.1.4.1.25623.1.0.100080	High	Moderate	Moderate
16	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	1.3.6.1.4.1.25623.1.0.105042	High	Moderate	Moderate
17	Anonymous FTP Login Reporting	1.3.6.1.4.1.25623.1.0.900600	Moderate		Low
18	Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check	1.3.6.1.4.1.25623.1.0.108011	High	Moderate	High
19	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	1.3.6.1.4.1.25623.1.0.111012	Moderate	Moderate	Moderate
20	Weak Host Key Algorithm(s) (SSH)	1.3.6.1.4.1.25623.1.0.117687	Moderate	Moderate	Moderate

Company B Cyber Security Tools

Company B has provided this list of cyber security tools in anticipation of being acquired by Company A. This list is assumed to be complete.

Table A. Cyber Security Tools

Tool Name	Purpose
Sophos/Intercept X	Endpoint Detection and Response
OneTrust	Data privacy/Data lifecycle management
Code42	Data-centric security
Sophos XG	Next-Gen Firewalls
No tool available	Mobile Device & Application Management
DUO	Identity and Access Management
Akamai	Application Security
Mimecast	Messaging Security
Arctic Wolf	Managed Security Services Provider
Cisco Umbrella	DNS Security
In progress	Cyber security policy
In progress	Written Information Security Policy (WISP)
In progress	Written procedures
Minimal	Documentation of environment

Company A Risk Analysis

Company A performed an internal risk analysis in anticipation of system integration with Company B. This risk analysis was performed in accordance with NIST SP 800-30 Rev 1 to identify the following:

- “Vulnerabilities”
- "Risk likelihood”

Table A. Risk Classifications

Risk Level	Description
High	The loss of confidentiality, integrity, or availability may be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The loss of confidentiality, integrity, or availability may be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Low	The loss of confidentiality, integrity, or availability may be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Table 1: Data Sensitivity

Type of Data	Sensitivity		
	Confidentiality	Integrity	Availability
Customer PII (e.g., Account Numbers, Social Security Numbers, and Phone Numbers)	High	High	Moderate
Employee PII (e.g., Social Security Numbers and Employee Identification Numbers)	High	High	Moderate
Company intellectual property (e.g., credit scoring calculations)	High	High	Moderate
Marketing and advertising	Moderate	Moderate	Low

Table C. System Inventory

System Components	
Servers	Windows server 2019; role: internal SharePoint server Windows server 2019; role: Exchange server Windows server 2012; role: Application server Windows server 2012R2; File server DMZ Windows server 2012; role: FTP and external Web Server
Workstations	75 - Windows 10 Pro 20 - configured for remote desktop access
Switches	4 - Cisco 3750X
Firewall	Fortinet's Fortigate 800D NGFW
Border router	Cisco 7600
Laptops	14 - Windows 7 6 - Windows 11
Wireless Access Points	2 - Meraki MR28
Cable plant	Cat5e

Table D. Risk Identification

Risk #	Vulnerability	Risk Likelihood
1	Open ports 21-90, 3389	High
2	All users use eight-character passwords	High
3	User accounts no longer required are not removed	Moderate
4	All users have local administrative privileges	Moderate
5	Regular password changes are not enforced	Moderate
6	End-of-Life Equipment in use	Low

Network and Merger Implementation Plan Solution

In order to begin with implementing a plan for the Merger we first need to consider some of the network security problems and infrastructure problems that both companies currently possess based of the above business requirements given in the scenario

Company A Network Security/Infrastructure problems

Company A deals with Sensitive customer information like checking accounts, bank cards, and investment products. Therefore there needs to be a big emphasis on Security controls that lowers the chances that a malicious actor can gain access to sensitive customer information. Because all users at Company A have local admin privileges this is a network security risk that leaves sensitive customer financial information at great risk due to the fact that a malicious actor external or internal could exploit this elevated privilege to have access to sensitive customer information. In that same breath the fact that the users also don't practice usage of strong passwords could make it very easy for an external threat actor to gain access to the company internal system to steal sensitive customer information. Company A also has weak access and identity management as they make no effort to delete inactive user accounts. They also make use of end of life software like Windows 7 which as of January 10 2023 marked the end of support for the operating systems which leaves customer information at a greater risk of getting exposed if new Windows 7 Vulnerabilities arise

Company B Network Security/Infrastructure problems

Company B poses more of a merger security risk in big part due to the fact that they dont have their own internal dedicated Cybersecurity team. For a company reliant on securing customer information They're more at risk since they are reliant on the security controls of the vendors they contract with. Part of the network security problems Company B possess that poses a high data risk leak to their customers is their lack of MFA(Multifactor Authentication). Given their heavy reliance on external vendors not having a DMZ(Demilitarized Zone) away from their important internal severs is also a high network security risk. A couple of infrastructure issues include the lack of least privilege as every company B user has admin prileges which in the medical software field poses high security risk. Their usage of end of lifes systems is risky too given the lack of security patches for new vulnerabilities that could arise.

Network Diagram/Vulnerability scan assessment for Company A

One of the existing vulnerabilities from Table D for Company A is Risk #1 in which ports 21-90, and 3389 Are left open. The likelihood that this vulnerability gets taken advantage of is high, especially given how many opened ports there are. It gives a threat actors a lot of options for how to gain access to the company's system and the impact If successfully exploited would lead to sensitive medical related customer data being leaked. One of the key security methodologies is to close every port and only unlock the ports needed. With the risk if not addressing this vulnerability being high will need to evaluate the need for each opened port and how truly needed they are for day to day functions with more emphasis place on using the secured versions of ports only.

Another existing vulnerability from Table D for Company A that would need to be addressed is Risk #3. The Risk likelihood of this occurring is moderate but the impact it could have is high given that the likelihood that a breached account possess admin privileges is also high based off Risk #4. The risk that a disgruntled employee would want to take revenge against the company is moderate but if the intel that old user accounts are not being properly deleted gets in the hands of a malicious threat actor they could offer monetary compensation which could entice the employee that otherwise would have never thought to exploit said vulnerability.

Network Diagram/Vulnerability scan assessment for Company B

One of the Vulnerabilities for Company B presented in Table E that would need to be addressed is risk #2 and risk #4 and risk #6 concurrently as they can be the catalyst for a data breach. This catalyst if it occurs affects one of the equipment's company B has listed in Table D, HPE JZ337A Aruba AP-535. This Severe vulnerability affects HPE JZ337A Aruba AP-535, in which a malicious actor has the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS. Due to the lack of Multi factor authentication a malicious actor would have an easier time breaking in and considering that all users have local administrative privileges, a malicious threat actor, could potentially exploit the above vulnerability in HPE JZ337A Aruba AP-535, therefore would need to ensure that the OS is updated to a version where this vulnerability is addressed. The individual likelihood of each of these risks being exploited are pretty moderate and being exploited consecutively knocks that likelihood down but the risk is still there and the impact of the fallout of each being exploited is of critical severity

Another Vulnerability is risk #8 Apache Tomcat which leaves the system prone to remote code execution vulnerability in the AJP connector. if exploited enables an attacker the ability to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code. There is a security patch that addresses this vulnerability. But the severity if exploited can lead to breach of customer data confidentially as well as integrity and also availability. The risk it poses is high but requires moderate effort to address

Proposed Merged Network Topology

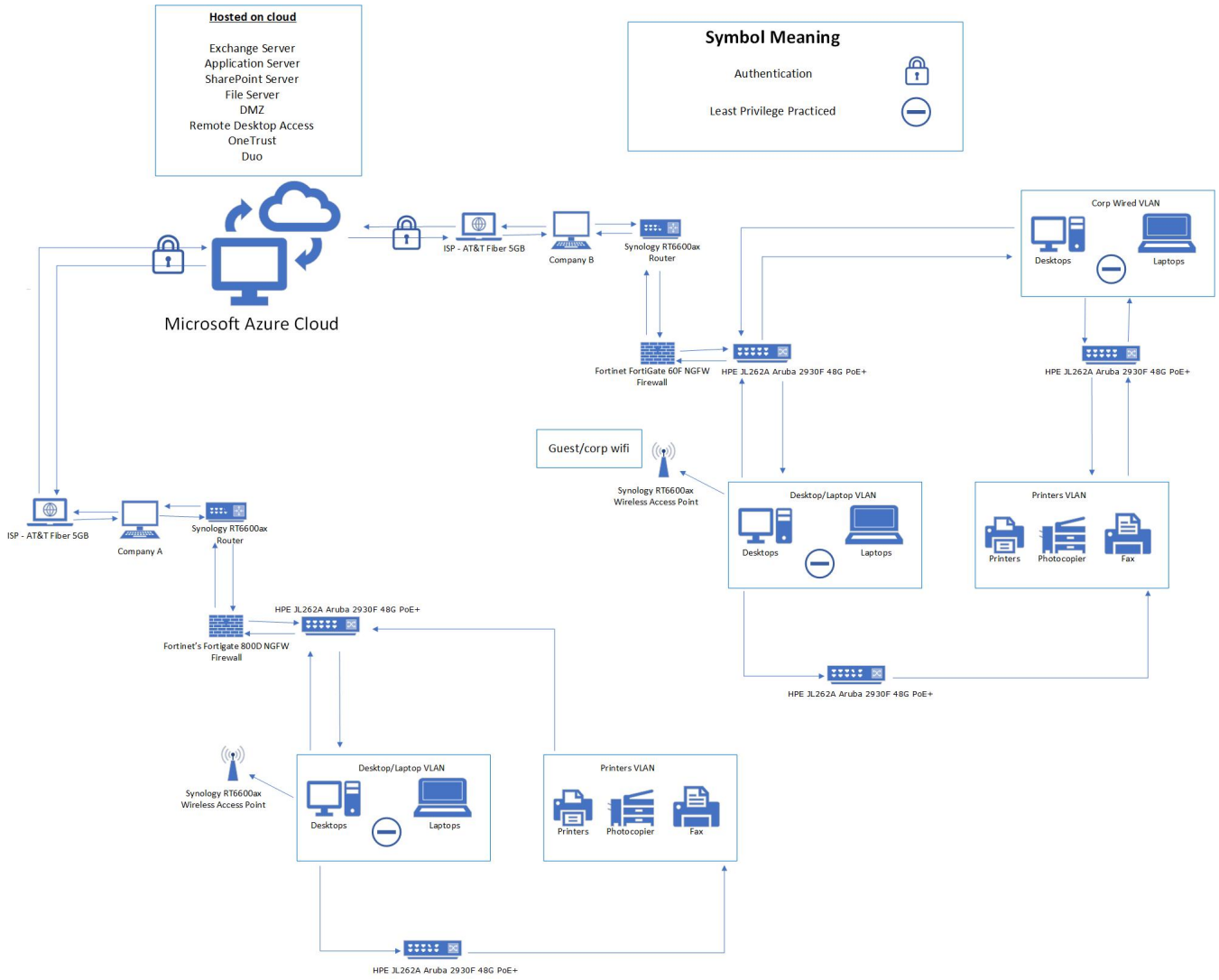

Figure 3: Merged Network Topology

Overview of selected Network Components/Topology

Table A. New Components selected

Component	Quantity	Cost	Total Cost
Microsoft 365 Business Standard	50	$12.50	$7500
DUO	50	$3/month	$1800/year
Synology RT6600ax router	2	$312	$624
HPE JL262A Aruba 2930F 48G PoE+	2	$1459	$2918
Fortinet FortiGate 60F NGFW Firewall	1	$367	$367
Microsoft Azure Virtual Machines	2	$462.39/Month	$5549/Year
Brother MFC-L8900CDW color laser all-in-one printer	2	$649.99	$1299.98
AT&T Fiber 5GB	1	$285	$1995
OneTrust GDPR Compliance Policy	1	$2275/month	$27300/year

Table B. OSI and TCP/IP of Network Components

Component	OSI Layer	TCP/IP Layer
Microsoft 365 Business Standard	7	4
DUO	7	4
Synology RT6600ax router	3	2
HPE JL262A Aruba 2930F 48G PoE+	2,3	1,2
Fortinet FortiGate 60F NGFW Firewall	3,4,7	2,3,4
Microsoft Azure Virtual Machines	7	4
Brother MFC-L8900CDW color laser all-in-one printer	All	All
AT&T Fiber 5GB	1	1
OneTrust GDPR Compliance Policy	7	7

The above network topology in Figure 3 comes out to $49352.98 with the newly added components, which is shy under the $50,000 budget given. This topology is a great scalable way to merge the networks of both company A/B, as a lot of the items that would prove to be difficult to address in this merger like the DMZ, and various servers are going from being managed in house or via an in house virtual machine to now all being hosted on the cloud, which lowers the implementation burden for this merger. Because Company A/B have a heavier Microsoft presence in their IT systems and the ease of use and many benefits it offers i opted to use Microsoft Azure as the Cloud Solution.

Due to budgetary constraints i did opt to lean more into a solution that addresses a lot of security concerns via regulatory laws. For example in my earlier plans i did want to increase the number of Windows 11 workstations and laptops as it is currently being supported long term versus Windows XP/7 which are currently at End of

life or will be very soon and will no longer be receiving active security updates to address new vulnerabilities. However, given the massive costs this would lead to i decided instead to keep all the workstations/laptops that each company already possesses and instead implement security controls that would see that high risk devices like Windows 7 Workstations and laptops not have admin privileges and are not used in a way where sensitive information is processed through those devices. Doing this gave more room in the budget for the addition of Cybersecurity tools like DUO, OneTrust from Company B's Cybersecurity tools table.
I did also drop using the Cisco 7600 router as that is also an End of life switch not receiving anymore support and instead opted for the Synology RT6600ax router. Added more of the Aruba Switches and with company B already having 3 stacked Aruba switches this helped offset some of the switch related costs. Sophos XG firewall is another End of life item that ended up getting cut from the final merged topology. So, i replaced that with a a well rated firewall in the Fortinet family which is also being used in Company As topology. Settled on AT&T as the ISP provider as their a reliable giant in the ISP service world and 5Gbs of speed will reduce the chances of availability issues occurring.
Based of both companys risk assessments a major issue in both seem to be a lack of multifactor authentication as well as a lack of commitment to zero trust/least privilege principles. In my topology i hoped to address these vulnerabilities the Lock signifying Duo Authentication and the Permission icon which signals that least privilege will be practiced in those networks.
A huge chunk of the budget is going towards OneTrust. This component addresses the following regulatory compliance requirements for this merger.

- "General Data Protection Regulation (GDPR) ",
- “Gramm-Leach-Bliley Act (GLBA)”,
- "California Consumer Privacy Act (CCPA)”

These 3 regulatory requirements are relevant and need to be met as the sector that both Companies operate in is finance related and deals with the ownership of sensistive customer financial information like Social Security numbers, Name, Address, credit card numbers etc. Onetrust offers pricing directly related to GDPR Compliance and also the CCPA. The GDPR compliance package that they offer covers the subset of packages that are also included in the CCPA compliance package. It also includes a Privacy rights automation which checks the box for the GLBA compliance policy. So, Because the above topology implements the GDPR Compliance policy via the cloud that covers the regulatory bases related to those 3 compliance policy.

While this Merged Network Topology is a more than a great baseline, there are still some potential issues issues to keep in mind. One of the potential issues to keep in mind relates to the workstations and laptops still using Windows 7/XP. These operating systems no longer receive any security support from Microsoft and many software and applications have been slowly fazing out security in relation to these operating systems. This makes them a very risky option to be used to conduct day to day business, especially given the sensitivity of the type of business that is being conducted at the merged company. The best solution is to completely phase out usage of these Operating systems. However, given budgetary concerns they could still be used just in very limited forms, for example as guest only accounts with limited user account access.

Another security concern relates to timely security patches. As seen from the lengthy vulnerability report

from company B, a lot of the vulnerabilities found were as a result of not applying security patches for known vulnerabilities with fixes. If these patches are not kept up with this merged topology would lose effectiveness. A solution that needs to be put in place to address this should be to form an internal CyberSecurity team to keep up with systems nearing end of life in order to make timely upgrades, as well as being in the know how of when a security vulnerability arises in one of the various areas in the network and applying security patches as soon as they are made available. This CyberSecurity team should also take the challenge of keeping in contact with the cloud vendor to ensure that the service level agreements made are consistently being adhered to especially given how reliant the system is on OneTrust in the cloud enforcing GLBA,GDPR, and CCPA regulatory compliance requirements

Benefits of a Cloud Solution in Merged Network Topology

Its easy to glance at the amount being invested into this Cloud solution. However, it's a worthwhile solution for various reasons. One of those reasons relates to how much neater and straightforwards a cloud implementation is for our network. It reduces clutter, overall labor and part costs that would have gone into ensuring an on premises solution for a DMZ, Enterprise Servers, etc. Had we chosen an on premise solutions We would need to either go above the budget or sacrifice equipment quality in order to be able to afford more equipments for an on premise solutions. This also increases cost as the new on premise solution would need more costly safeguards put in place

The Security compliance that OneTrust provides also is nonnegotiable. It ensures that we are GPDR,CCPA, and GLBA compliant. OneTrust takes on the burden of ensuring that the company Remains compliant with GDPR, GLBA, and CCPA. The costs of ignoring these regulatory compliance's are high as the GDPR itself "gives supervisory authorities the power to issue fines of up to €20 million or 4% of an organisation's global annual turnover"(Irwin Luke,2023). It doesn't stop at just the fines also as it's found that organizations spend about "€3.94 million responding to a data breach"(Irwin Luke,2023). "On average, small- and mid-sized organizations can expect to spend more than $100,000 to get and stay compliant with GDPR. Larger organizations can expect to spend even more"(Secureframe n.d.). In contrast $27300 pales in comparisons to the the amount most companies are spending to be within this regulatory compliance.

References

Irwin, Luke. "How Much Does GDPR Compliance Cost in 2023?" IT Governance Blog En, May 10, 2023. https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020.

Secureframe. "The Cost Benefits of GDPR Compliance Automation." Secureframe. Accessed June 16, 2024. https://secureframe.com/hub/gdpr/cost-and-time-savings.

"CVE-2022-37888 Detail." NVD. Accessed June 16, 2024. https://nvd.nist.gov/vuln/detail/CVE-2022-37888.

"CVE 1.3.6.1.4.1.25623.1.0.143545." Web application abuses: Apache Tom-

cat AJP RCE Vulnerability (ghostcat). Accessed June 16, 2024. http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.143545.

Arctic Wolf. "Financial Institutions Regulatory Checklist." Arctic Wolf, May 23, 2024. https://arcticwolf.com/resources/blog/a-simplified-regulatory-checklist-for-financial-institutions/.

Amazon.com: Hp newest 15.6" FHD Essential Business Laptop, Intel core i5-1135G7 processor, 32GB RAM, 1TB storage, Intel Iris XE graphics, SD Card Reader, HDMI, Ethernet, Webcam, USB-C, Windows 11 Pro: Electronics. Accessed June 17, 2024. https://www.amazon.com/HP-Essential-Business-i5-1135G7-Processor/dp/B0CT98X2CV.

Windows 11 Pro for Workstations (download). Accessed June 17, 2024. https://www.microsoft.com/en-us/d/windows-11-pro-for-workstations/dg7gmgf0kr4m.

Amazon.com: Customer reviews: Synology RT6600AX - tri-band 4x4 160mhz wi-fi router, 2.5Gbps ethernet, VLAN segmentation, multiple ssids, parental controls, threat prevention, VPN (US version). Accessed June 17, 2024. https://www.amazon.com/product-reviews/B09ZQ5W4G7 ref=cm_cr_dp_mb_top.

Amazon.com: Fortinet Fortigate 60F hardware – next-gen firewall protection & security: Electronics. Accessed June 17, 2024. https://www.amazon.com/Fortinet-FortiGate-Firewall-Throughput-Protection/dp/B07ZZMFWJ7.

Imgur. "Microsoft Azure Estimate." Imgur. Accessed June 16, 2024. https://imgur.com/a/Ag2SGmT.

"Brother MFCL8900CDW: Business Color Laser All-in-One Printer with Low-Cost Printing." Brother MFCL8900CDW | Business Color Laser All-in-One Printer with Low-Cost Printing. Accessed June 16, 2024. https://www.brother-usa.com/products/mfcl8900cdw?srsltid=AfmBOoptP29m6e4VsINXjlrW9Kj98vblFlX776nglAWQVKMEuk7kYZwaNQA.

Amazon.com: Hp HPE Aruba 2930F 48G poe+ 4SFP switch, JL262A: Electronics. Accessed June 17, 2024. https://www.amazon.com/HP-Aruba-2930F-Switch-JL262A/dp/B01HPKW7GM.

Osman Husain. "OneTrust Pricing: How Much Does OneTrust Cost? [2024 Figures]." Data Privacy Compliance Software for Apps, Websites, & SaaS, June 16, 2024. https://www.enzuzo.com/blog/onetrust-pricing-for-compliance.

"Compare Microsoft Exchange Online Plans Microsoft 365." Compare Microsoft Exchange Online Plans Microsoft 365. Accessed June 16, 2024. https://www.microsoft.com/en-us/microsoft-365/exchange/compare-microsoft-exchange-online-plans.

"AT&T Business Fiber®: High Speed Business Fiber Internet Service." AT&T Business. Accessed June 16,

2024. https://www.business.att.com/products/business-fiber-internet.html.