DECEMBER 7, 2023

KINGSLEY SAMUEL

NETWORK MERGER AND IMPLEMENTATION PLAN

TABLE OF CONTENTS

SUMMARY

Merged networks have become increasingly more prevalent in the business world. This report emphasizes the critical importance of designing a secure and compliant network infrastructure for such organizations. The presented network topology represents the minimum required configuration for regulatory compliance within budget constraints. However, a layered defense-in-depth approach is recommended for optimal security posture. While implementing additional security measures, such as software-based IDS/IPS or comprehensive cloud migration, would incur upfront or ongoing costs, these investments can be offset by their long-term benefits. Cloud-based infrastructure, for example, offers cost-effective scalability and flexibility, while on-premise solutions provide greater administrative control. Based on a cost-benefit analysis and industry best practices, transitioning to a cloud-based architecture appears to be the most functional solution for this organization.

The proposed network design recommendation includes adding layers of defense through the addition of Next Generation Firewalls, IDS/IPS, network segmentation and providing cost-effective scalability through cloud computing. By implementing this design, the company can save costs by consolidating the network, reducing the need for additional infrastructure and resources. This will ensure that the company doesn't exceed

its first year budget of $50,000. Furthermore, managing a single network rather than two separate networks will increase operational efficiency, reduce complexity, and maintenance costs. Additionally, the unified network and cloud computing will allow for accommodating additional users, services, and devices, leading to less complication. This report also outlines various compliance measures, including defense-in-depth implementation, proper documentation, and robust security policies. These measures statisfies the executive requirement of developing a scalable and redundant network centralized on a zero-trust principal with the utilization of both on premise and cloud infrastructure. With diligent maintenance and proactive patching, this proposed network topology should provide adequate security for the company's assets and operations.

NETWORK SECURITY AND INFRASTRUCTURE PROBLEMS

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."

Considering the upcoming merger between Company A and Company B, it is crucial to assess the existing security measures in place for both entities. Company A operates within the financial sector, where safeguarding customer Personally Identifiable Information (PII) is of utmost importance. Meanwhile, Company B, though smaller in size, lacks an in-house cybersecurity team and relies on third-party support for its infrastructure. Additionally, Company B processes credit card payments and offers software solutions to medical providers.

Company A has placed a high priority on confidentiality and integrity, with a moderate level of concern for availability. However, based on a risk analysis, it appears that there are multiple major network security concerns within the company. This includes the discovery of multiple open ports 21 - 90, 3389, and the fact that all users have local administrative privileges. Further investigation reveals that the current infrastructure problems are decreasing the overall security of Company A, with the usage of end-of-life equipment and a lack of endpoint detection and response (EDR) putting the company's security at risk.

Meanwhile, Company B's vulnerability report and cybersecurity tools reveal several network security concerns, including the SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability and rsh unencrypted cleartext login. The report also highlights areas of infrastructure that require attention, such as the absence of tools for mobile device and application management, the lack of written cybersecurity policies, and insufficient documentation.

In light of these findings, it is clear that both Company A and Company B require significant improvements in their network security and infrastructure. This is crucial in order to safeguard customers' personally identifiable information prior to the merger.

EXISTING VULNERABILITIES AND IMPACT

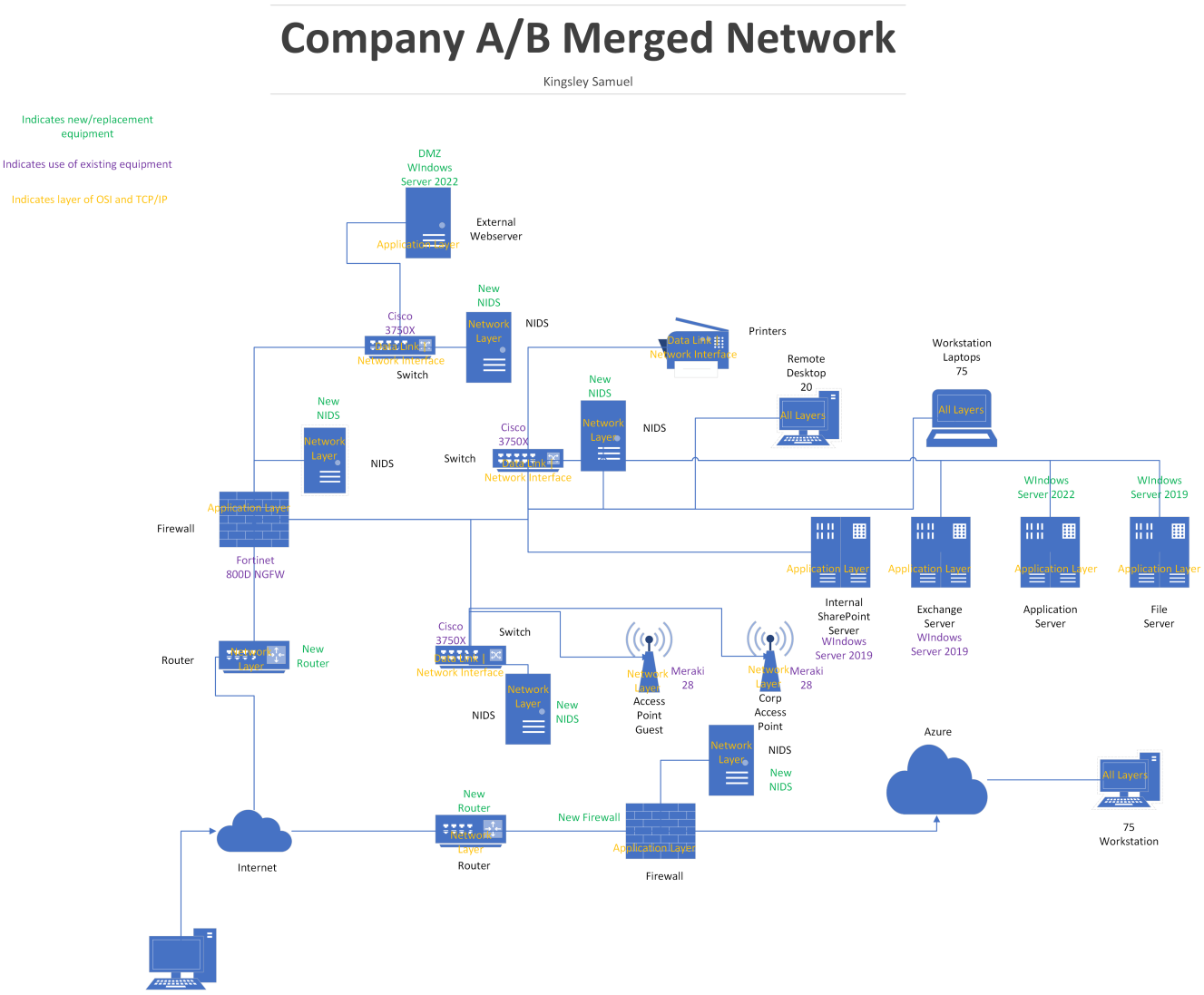
Upon close examination of the risk analysis and network diagram of Company A, it has become evident that there are several vulnerabilities that require immediate attention. One of the most significant vulnerabilities is the exposure of open ports 21-90 and 3389 as identified in Table D of the Risk Identification report. It is highly recommended to keep unused ports closed to minimize the attack surface for potential threats. If these vulnerabilities remain unaddressed, cybercriminals could exploit them to gain unauthorized access to sensitive data and personally identifiable information (PII). This is especially concerning given Company A's position in the financial industry and its compliance with GDPR and PCI DSS regulations. The likelihood of such an event occurring is alarmingly high, which could result in a significant risk to the confidentiality, integrity, and availability of information.

Another vulnerability that was discovered is the password policy and the use of eight-character passwords. This policy leaves user accounts vulnerable to brute force attacks, which could lead to the compromise of essential information such as customer PII, employee PII, and company intellectual property. The likelihood of such an event occurring is high, which could result in a catastrophic adverse effect on the company's operations, organizational assets, and individuals.

Similar to Company A, Company B also suffers from vulnerabilities that could compromise its cybersecurity. Upon conducting a thorough analysis of Company B's vulnerability report and cybersecurity tools, it was discovered that the company has outdated equipment and unpatched devices, making it vulnerable to many exploits. This poses a significant risk to sensitive data such as credit card payment information and could disrupt the company's operations. Due to the high number of unpatched systems, the likelihood of a security event is quite high, further increasing the risk of data being compromised.

Furthermore, the vulnerability report and cybersecurity tools reveal a severe lack of documentation and formal security procedures within Company B. The company's lack of dedicated cybersecurity personnel has resulted in a lack of formal procedures for its employees, and no action plan in the event of a security breach. This vulnerability could lead to a data breach, improper data collection, and severe costs due to failing to follow PCI DSS. Given the critical role of documentation and proper policies in any organization, the likelihood of an event occurring is high, resulting in a high risk. Failure to address this vulnerability could lead to monetary loss and a compromise in data integrity.

NETWORK TOPOLOGY



EQUIPMENT	EQUIPMENT TYPE	QUANTITY	OSI | TCP	COST (USD)/Per Unit
Cisco A9KV-V2-AC	Router	2	Network Layer | Network Layer	$2,500.00
Cisco ASA5508-K9	Firewall	1	Application Layer | Application Layer	$1,190.00

EQUIPMENT	EQUIPMENT TYPE	QUANTITY	OSI | TCP	COST (USD)/Per Unit
Fortinet 800D NGFW	Firewall	1	Application Layer | Application Layer	$0.00
Snort IDS/IPS	Software	4	Network Layer | Network Layer	$399.00/(Annual)
Cisco 3750X	Switch	3	Data Link | Network Interface	$0.00
Meraki 28	Access Point	2	Network Layer | Network Layer	$0.00
Windows Server 2019	Server	2	Application Layer | Application Layer	$0.00
Windows Server 2022	Server	3	Application Layer | Application Layer	$1069.00
Workstation	Desktop/Laptops	170	Application Layer | Application Layer	$0.00
Azure	Cloud Services	75	Application Layer | Application Layer	$443.00/(Month)
Cat6	Cable	-	Physical Layer | Network Interface	$0.60/(ft)

Numerous factors were thoughtfully considered when devising the network topology for the merged networks of Company A and Company B. These included retiring outdated equipment, addressing well-known vulnerabilities, and incorporating cloud functionality, which necessitated several adjustments to the network.

Fortunately, reusing many of the workstations, laptops, desktops, printers, and wireless access points from Company A, along with Company A's Cisco 3750x switches and NGFW, as well as Company B's 2019 Windows servers, helped to keep costs down. However, we also introduced new hardware, such as updated windows servers, Snort

NGIDS, Cisco 9000 series routers, and Azure cloud services, to optimize the network's performance, security, and efficiency.

Windows Server 2022 is Microsoft's leading server product, ensuring that patches and updates are readily available and supported within the network. The Snort NGIDS, a Cisco product, functions in nodes and monitors network traffic alongside each switch in the company's network, allowing for early detection of intrusions.

The Cisco A9KV-V2-AC is Cisco's recommended generation of routers, offering network protection and flexibility in network consumption for stable network connectivity. Finally, the hybrid approach to network design, which includes services from Azure, is the ultimate addition. This affords seamless scalability, infrastructure security, and redundancy within the company network, while significantly reducing the cost of investing in new network devices and keeping the new network infrastructure well under the $50,000 budget set.

SECURE NETWORK DESIGN PRINCIPLES

Various secure network design principles exist that organizations can follow to ensure they are resilient to different types of threats. To this end, I have developed a network topology for the merged company that incorporates many principles, including defense in depth and segmentation.

The principle of defense in depth involves implementing multiple layers of security controls to diminish the risk of a security breach and heighten the probability of detecting and responding to potential threats. The network topology diagram displays the multiple layers of defense utilized as connectivity traverses further within the network. The first layer of defense entails a firewall, followed by an IDS on every switch within the network. This enables another principle, visibility, which allows the organization to scrutinize, evaluate, and track the network and identify potential threats.

Moreover, dividing the network into smaller sections or zones limits the impact of a security breach. Partitioning areas like the DMZ and access points from other areas of communications lessens the risk of security breaches in other parts of the network.

REGULATORY COMPLIANCE

As previously mentioned, Company A operates in the financial industry and is required to comply with several laws and regulations due to the nature of their transactions. This includes GDPR, a European Union data regulation that mandates the protection of EU customer privacy by enforcing specific standards. In the case of our new merged network, GDPR compliance will be maintained through network segmentation and a robust defense mechanism. This ensures that if the network is compromised, the breach will be detected before it reaches critical PII.

PCI DSS is another regulation that Company A must comply with when handling cardholder data. The company ensures compliance by implementing policies that address security for all personnel, including encryption, least privilege, user awareness training, incident management, risk assessment, patching, and updates.

On the other hand, Company B provides services to medical providers and is therefore required to comply with HIPAA. This regulation ensures the confidentiality, integrity, and availability of all protected health information. The merged company will be in compliance with GDPR, PCI DSS, and HIPAA, thanks to the network design infrastructure that includes authentication and access control, configured firewalls and VPNs, encryption, and segmentation.

RECOMMENDATION AND IMPLEMENTATION

To ensure network security, it is not enough to have a well-designed network topology. Organizations should adopt a proactive approach that goes beyond technical implementation. This includes enforcing strong security policies, keeping systems up-to-date with patches, and promoting security awareness among employees.

Although the presented network topology meets regulatory minimums, it is complex and can be vulnerable to misconfigurations. This complexity can hinder the effectiveness of traditional defense-in-depth approaches, which rely on multiple layers of security. For smaller organizations, implementing and maintaining such a comprehensive framework can be challenging.

An alternative approach is transitioning to a zero-trust security model. This model eliminates implicit trust and continuously verifies the identity and authorization of users and devices before granting access to resources. This approach simplifies security management and reduces the overall cost and administrative burden. However, it is crucial to consider the specific implementation challenges and provide proper training to personnel.

Inadequate network management poses another significant risk. Rigorous patch management, proactive vulnerability identification, and traffic monitoring are necessary to mitigate threats. Implementing documented policies and procedures for network management, combined with employee training on cybersecurity best practices, can significantly reduce the risk of network compromise and ensure data confidentiality, integrity, and availability.

REFERENCE

End-of-Sale and End-of-Life Announcement for the Cisco Service. Cisco. https://www.cisco.com/c/en/us/products/collateral/wireless/7600-wireless-security-gateway/eos-eol-notice-c51-736397.html

Cisco ASA5508-K9. ServerSupply. https://www.serversupply.com/NETWORKING/SECURITY%20APPLIANCE/FIREWALL/CISCO/ASA5508-K9_244933.htm?gad_source=1&gclid=Cj0KCQiAyeWrBhDDARIsAGP1mWQ7NYbxuiStXcBB-n7Oer12VPq-PZ3GR_3ZruYVSs35AOid774HEfQaAhe8EALw_wcB

https://www.vibrant.com/Cisco-A9KV-V2-AC.html

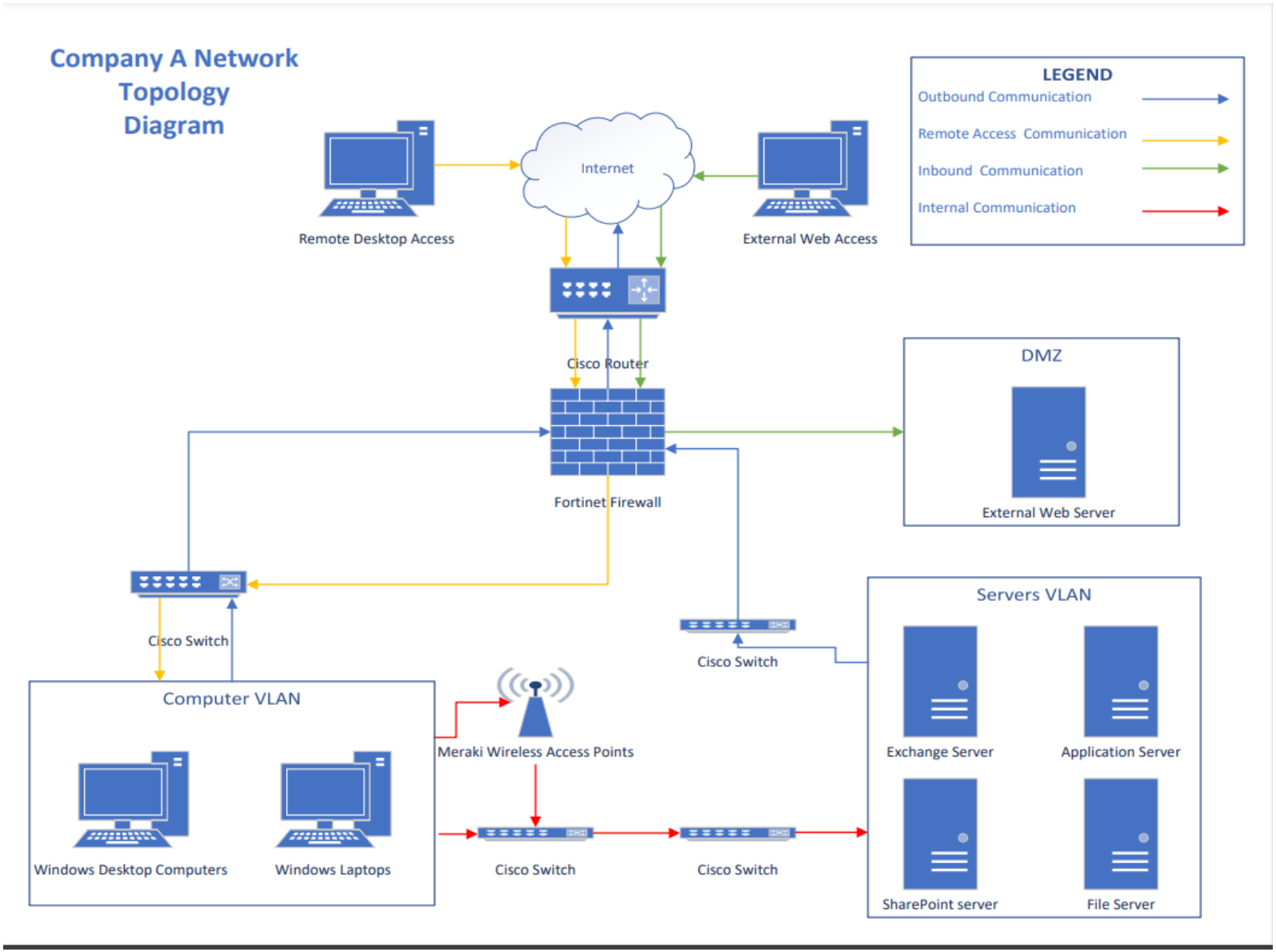
Snort Products. Snort. https://www.snort.org/products

Four Strategic Principles of Network Security Design. (2021). https://secureops.com/blog/network-security-design-four-principles/

GRC International Group. (n/d). *Governance and Regulatory Compliance*. https://www.itgovernanceusa.com/compliance

Hiter, S. (2021, Sept 8). *Five Tips for Managing Compliance on Enterprise Networks*. https://www.enterprisenetworkingplanet.com/standards-protocols/compliance-management-enterprise-networks/

Merchant resources. (2023, January 30). PCI Security Standards Council. https://www.pcisecuritystandards.org/merchants/#resources


Company A Network Topology Diagram
LEGEND
Outbound Communication
Remote Access Communication
Inbound Communication
Internal Communication
Internet
Remote Desktop Access
External Web Access
Cisco Router
Fortinet Firewall
DMZ
External Web Server
Cisco Switch
Cisco Switch
Servers VLAN
Exchange Server
Application Server
SharePoint server
File Server
Computer VLAN
Windows Desktop Computers
Windows Laptops
Meraki Wireless Access Points
Cisco Switch
Cisco Switch

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 B. Data Sensitivity

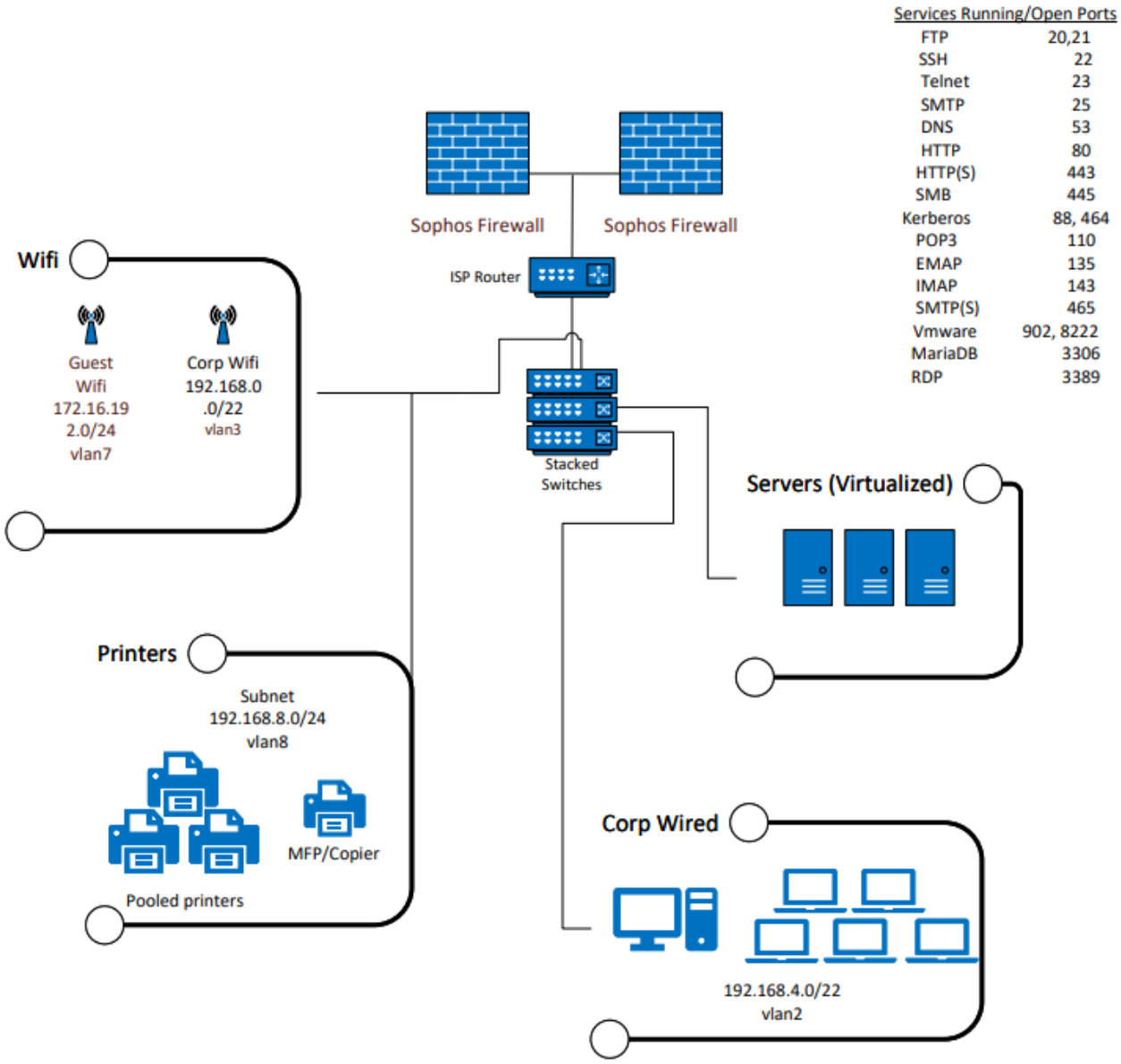
Type of Data	Sensitivity		
	Confidentiality	Integrity	Availability
Customer PII (e.g., Account Numbers, Social Security Numbers, and Phone Numbers)	High	High	Moderate
Employee PII (e.g., Social Security Numbers and Employee Identification Numbers)	High	High	Moderate
Company intellectual property (e.g., 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 800D NGFW
Border router	Cisco 7600
Laptops	14 - Windows 7 6 - Windows 11
Wireless Access Points	2 - Meraki M28
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


Services Running/Open Ports
FTP 20,21
SSH 22
Telnet 23
SMTP 25
DNS 53
HTTP 80
HTTP(S) 443
SMB 445
Kerberos 88, 464
POP3 110
EMAP 135
IMAP 143
SMTP(S) 465
Vmware 902, 8222
MariaDB 3306
RDP 3389
Sophos Firewall
Sophos Firewall
ISP Router
Wifi
Guest Wifi 172.16.19 2.0/24 vlan7
Corp Wifi 192.168.0 .0/22 vlan3
Stacked Switches
Servers (Virtualized)
Printers
Subnet 192.168.8.0/24 vlan8
MFP/Copier
Pooled printers
Corp Wired
192.168.4.0/22 vlan2

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

10	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

Microsoft Azure Estimate

Your Estimate

Service category	Service type	Custom name
Compute	Virtual Machines	
Databases	Azure SQL Database	
Identity	Azure Active Directory External Identities	
Support		

Disclaimer

All prices shown are in United States – Dollar ($) USD. This is a summary estimate, not a c
This estimate was created at 12/13/2023 7:25:18 PM UTC.

Region	Description
East US	1 D2 v3 (2 vCPUs, 8 GB RAM) x 730 Hours (Pay as you go), Windows (AHB), OS Only; 0 managed disks – S4; Inter Region transfer type, 5 GB outbound data transfer from East US to East Asia
East US	Single Database, vCore, General Purpose, Provisioned, Standard-series (Gen 5), Locally Redundant, 1 - 2 vCore Database(s) x 730 Hours, 32 GB Storage, RA-GRS Backup Storage Redundancy, 0 GB Point-In-Time Restore, 0 x 5 GB Long Term Retention
West US	Premium P1 tier: 50,000 monthly active user(s)
Support	
Licensing Program	Microsoft Customer Agreement (MCA)
Billing Account	
Billing Profile	
Total	

quote. For up to date pricing information please visit https://azure.microsoft.com/pricing/calc

Estimated monthly cost	Estimated upfront cost
$70.08	$0.00
$372.97	$0.00
$0.00	$0.00
$0.00	$0.00
$443.05	**$0.00**

culator/