2/2/2024

**Inomancy Home Care: Home Health Care Network Analysis**

*We’re Here for Life, We’re Here for You*

Liaison: : Inno Azuogalanya-Owner & Ike Azuogalanya-Assistant

Date prepared: March 11th 2024

Team Name: Team One

Each of our names here:

Olivia Barr

Naiya Whitely

Josiah Williams

Olivia Odugba

Anthony Azuogalanya

Sam Naim

Company Network Report

Contents

[**Executive Summary** 3](#_Toc163606261)

[**Organization Information** 4](#_Toc163606262)

[Company Name: 4](#_Toc163606263)

[Project Name with Scope: 4](#_Toc163606264)

[Liaison Name, Title, Mailing Address 4](#_Toc163606265)

[Data and Evidence – Team members 4](#_Toc163606266)

[Liaison Approval: 4](#_Toc163606267)

[**Business Scenario** 5](#_Toc163606268)

[Business Overview: 5](#_Toc163606269)

[Report Purpose: 5](#_Toc163606270)

[IT Governance Structure: 5](#_Toc163606271)

[Enterprise Architecture and Project Scope: 6](#_Toc163606272)

[**Current Network** 7](#_Toc163606273)

[Description: 7](#_Toc163606274)

[Hardware: 7](#_Toc163606275)

[Software: 8](#_Toc163606276)

[**Needs Assessment** 8](#_Toc163606277)

[**Risk Assessment** 9](#_Toc163606278)

[Risk Measurement Criteria: 10](#_Toc163606279)

[Inventory IT Assets: 10](#_Toc163606280)

[Identify Threats: 11](#_Toc163606281)

[Document Existing Controls: 12](#_Toc163606282)

[Identify Improvements: 12](#_Toc163606283)

[**Target Network** 15](#_Toc163606284)

[Recommended Physical Network: 15](#_Toc163606285)

[Recommended Logic Network: 16](#_Toc163606286)

[Gap Analysis: 17](#_Toc163606287)

[SWOT Analysis: 17](#_Toc163606288)

[Product Recommendations: 17](#_Toc163606289)

[**Migration Overview** 18](#_Toc163606290)

[**Conclusion** 20](#_Toc163606291)

[**Appendix** 21](#_Toc163606292)

[Appendix A - IT Governance Structure 21](#_Toc163606293)

[Appendix B - Enterprise Architecture 22](#_Toc163606294)

[Appendix C – Risk Assessment with Original Setup 23](#_Toc163606295)

[Appendix D – Risk Assessment with Recommended Setup 24](#_Toc163606296)

[Appendix E - Current Infrastructure Cost 25](#_Toc163606297)

[Appendix F – Identify Threats 26](#_Toc163606298)

[Appendix G – Identify Threats 27](#_Toc163606299)

[Appendix H – Recommended Physical Network 28](#_Toc163606300)

[Appendix I – Target Infrastructure Cost 29](#_Toc163606301)

[Appendix J – SWOT Analysis 30](#_Toc163606302)

[Appendix K – Recommended Logical Network 31](#_Toc163606303)

[Appendix L – Current Physical Network 32](#_Toc163606304)

[Appendix M – Current Logical Network 33](#_Toc163606305)

[Appendix N – Gap Analysis 34](#_Toc163606306)

[Appendix N – Gap Analysis 35](#_Toc163606307)

# **Executive Summary**

Inomancy Home Health Care, a small business providing essential medical supplies and a one-stop medical store, is set up to enhance its network security to safeguard confidential client and employee information. Recognizing the importance of data integrity and secure operations, the proposal includes the integration of Virtual Private Networks (VPNs), two-factor authentication, and access controls tailored to specific employees. This initiative aims to secure sensitive data across both home supply services and in-store transactions, ensuring the confidentiality and reliability of their client interactions. By reinforcing its network architecture, Inomancy Home Health Care commits to delivering a better service while creating a trustworthy and loyal environment among its clientele. Ultimately the goal is to better both the security and the operational efficiency of the business.

# **Organization Information**

## Company Name:

Inomancy Home Health Care & Inomancy Health Care store

## Project Name with Scope:

Inomancy Home Care: Home Health Care Network Analysis Scope

## Liaison Name, Title, Mailing Address

Inno Azuogalanya (Owner)

Ike Azuogalanya (Assistant)

## Data and Evidence – Team members

**­**Sam Naim

Olivia Barr

Naiya Whitley

Josiah Williams

Olivia Odugba

Anthony Azuogalanya

## Liaison Approval:

We want to work with the Inomancy Home Care Inc. network environment. We need your signature to approve us doing this work and working alongside the business to find their needs. This project is just a recommendation for what the business can do with its network and ways it can be better.

Liaison Name: \_\_Ike Azuogalanya\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_Ike Azuogalanya\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_03/12/2024\_\_\_\_\_\_\_\_\_

# **Business Scenario**

## Business Overview:

Inomancy Home Health Care is a small business that provides medical supplies to clients and nurses if needed. These medical supplies could be wheelchairs, electrical beds, canes, walkers, gloves, hand sanitizer, and much more. The company serves clients who go through insurance and doctors to be able to receive monthly drop-offs of small necessities like diapers, medical drinks, and other things. In some instances, clients or customers will need a larger item such as a wheelchair or another product, and Inomancy can deliver these as well. Another aspect of the company is the medical store, which is a one-stop shop for customers to buy all their needs and necessities in person. The store sells all the same products with a couple of additions such as scrubs, casts, crutches, and more. The store allows customers to get the supplies they need without having to go through insurance or doctors, which can make things a lot easier for the customer. Many times, people come in for a family member who has a need, and they can pay for it in cash or some form of insurance. For this project, we will be using the network systems for both the medical store and home supplies.

## Report Purpose:

The scope of our project is assessing Inomacy Health Care’s network architecture risk to ensure confidential client and employee information is secure. We aim to do this by adding VPNs, two-factor authentication, and limiting access to only certain employees. We will be evaluating user permissions and access through the client portal. This entails analyzing the company’s network throughout the OSI model, specifically layer 3 (Network).

## IT Governance Structure:

The company is a family-owned business with the father, Inno Azuogalanya, being the owner. Under Inno is his son, Ike Azuogalanya running much of the operational work for the business. Significant financial decisions and strategic directions under the guidance of the owner, Inno. Day-to-day operational decisions are made by Ike. The company has a manager to oversee the staff and overall oversight during work hours. Lastly, there is an IT analyst that works as a contractor to handle any IT needs. **Appendix A:**

## ­Enterprise Architecture and Project Scope:

A diagram of the current setup can be found in **Appendix B**.

The project proposal aims to enhance the network infrastructure of Inomacy Health Care, focusing on mitigating risks to safeguard confidential client and employee data. Key strategies include the integration of a Virtual Private Network, the adoption of two-factor authentication, and strict access controls to ensure that only authorized personnel can access sensitive information. Our assessment will scrutinize user permissions and the security of the client portal, with an emphasis on the network's design, particularly at the OSI model's layer 3.

The tangible outcomes of this project are multifaceted. Firstly, it will secure client information more effectively, preventing unauthorized access and potential data breaches. Implementing a firewall will further enhance network security, creating another layer of security against external threats. The proposal also includes upgrading the payment processing systems to be both flexible and secure, alongside enhancing the Point of Sale (POS) system, which will improve operational efficiency.

On the intangible side, the project is expected to deliver significant value by reducing customer Average Wait Time (AWT), thereby enhancing the overall customer experience and satisfaction. This improvement, coupled with increased data security, is anticipated to increase customer retention rates and foster greater trust and loyalty towards Inomacy Health Care. Additionally, the upgrades will contribute to creating a more productive and efficient workspace for employees, enabling them to perform their roles more effectively.

# **Current Network**

## Description:

The current network setup is a basic Local Area Network (LAN) primarily composed of 15 desktop computers connected through wired connections. These devices are connected to the internet via a modem and router, without the use of an additional network switch. This setup currently does not support Virtual Private Networks (VPNs), lacks file restrictions, and has no access controls in place. Peripheral devices include standard office equipment such as a telephone system, fax machine, and a multi-function office printer. There are no VOIP phones or specialized network hardware beyond the basic modem/router unit. The network's simplicity suggests minimal differentiation between user access levels and does not currently support remote or secure access protocols.

## Hardware:

|  |  |
| --- | --- |
| Desktop Computers: 15x Dell OptiPlex 3080 Micro | Compact, cost-effective desktops that are suitable for office tasks. |
| Modem and Router: TP-Link Archer C1200 | A reliable, budget-friendly combo unit that provides adequate internet access for a small office network. Modem is provided by AT&T. |
| Printer: Brother MFC-L2710DW | An affordable multi-function laser printer that offers printing, scanning, copying, and fax capabilities, ideal for small office needs. |
| Telephone System: Panasonic KX-TGF352N Corded/Cordless 2 Handset Landline Telephone | An economical choice for small businesses needing a reliable phone system with multiple handsets. |
| Fax Machine: | Included with the brother MFC-L2710DW multi-function printer, eliminating the need for a separate fax machine unit. |

## 

## Software:

|  |  |
| --- | --- |
| Operating System: Windows 11 Professional | Provides the necessary features for business use. Remote desktops are currently in use for work from home employees. |
| Office Suite: Microsoft Office 365 Business Standard | A subscription-based service that includes access to Office applications plus OneDrive for business cloud storage. |
| Antivirus: Windows Defender | This is a free product that comes with the Windows OS |
| Network Management | Windows built-in network management tools for setting up and managing the network. |

# **Needs Assessment**

The current network infrastructure at Inomancy Health Care requires comprehensive upgrades to meet modern security, data management, and performance standards. Here's an expanded needs assessment with specific product recommendations:

Improved Security: The network's lack of advanced security measures such as VPNs and two-factor authentication leave it vulnerable to cyber threats. Implementing a robust security solution like Fortinet FortiGate Next-Generation Firewall would provide comprehensive protection, including VPN capabilities, intrusion prevention, and advanced threat detection. Additionally, enabling two-factor authentication with a service like Duo Security can significantly enhance access security, ensuring that only authorized users can access sensitive systems and information. The cost of Fortinet with its hardware will come to about $2500. The cost of Duo Security will be roughly $3 per staff member at the company.

Database and File Server: The absence of a dedicated server for databases and file management limits efficient data handling and security. Deploying a Dell PowerEdge T40 server as a dedicated file and database server would centralize data storage, allowing for better management, enhanced access control, and simplified backup and recovery processes. This server choice is budget-friendly and scalable, suitable for small to medium-sized healthcare providers. This will be a one-time cost of $1800 which may save money from having to pay for Microsoft cloud services.

Upgrade Hardware: The current setup with basic desktops, a modem-router combo, and minimal peripherals is insufficient. Upgrading the network with a $1000 Cisco Catalyst 2960-X Series Switches will enable more efficient data traffic management and support for advanced security features. Replacing the existing desktops with HP EliteDesk 800 G5 Mini PCs would provide a more powerful computer environment, but this may be a want more so than a need. Additionally, introducing Aruba Instant On AP22 Wi-Fi access points would offer secure and reliable wireless access.

MAC Address Filtering: To enhance network access security, implementing MAC address filtering would ensure that only approved devices can connect to the network. This layer of security prevents unauthorized devices from accessing sensitive information, significantly reducing the risk of data breaches. Configuring these devices to recognize and permit only known MAC addresses adds an essential security measure, especially in environments dealing with confidential health information.

Incorporating these specific hardware and software upgrades into Inomancy Health Care's network will address the current limitations and vulnerabilities, significantly improving security, data management, and overall network performance. This strategic investment in technology will enable the healthcare provider to better serve its clients and protect sensitive information in an increasingly digital and connected world.

# **Risk Assessment**

The risk assessment process for the organization is to help understand the various potential vulnerabilities and threats that could compromise our IT infrastructure. This evaluation involves not only the identification of potential threats but also an analysis of their current security measures' effectiveness in mitigating these risks. It helps in highlighting gaps in their existing infrastructure. This strategy encompasses a blend of technical controls, such as firewalls, encryption, and access controls, alongside organizational measures like staff training and policy development. The ultimate goal of this risk assessment is to look for potential security breaches and ensure there is a plan for maintaining the data and the systems. **Appendix C** shows an example of the current risk assessment. **Appendix D** shows an example of a risk assessment for the proposed changes.

## Risk Measurement Criteria:

* Financial Impact: Evaluates the potential financial loss resulting from cybersecurity incidents, including data breaches, system downtime, and compliance penalties by the government.
* Reputational Impact: Assesses how security incidents could affect the organization's reputation among current customers, future clients, partners, and the industry.
* Operational Impact: Measures the extent to which business operations could be disrupted due to IT security threats. This will include the risk of phished credentials, ransomware, and other malware.
* Legal and Compliance Impact: Considers the legal ramifications and fines associated with failing to protect data or comply with industry regulations.

## Inventory IT Assets:

**Appendix E** will show the costs of the current infrastructure.

**Hardware:**

1. Desktop Computers:
   * Model: 15 Dell OptiPlex 3080 Micro
   * Processor: Intel Core i5-10500T (6 Cores/12 Threads, 2.3GHz to 3.8GHz)
   * Memory: 16GB DDR4 RAM
   * Storage: 256GB SSD
   * Operating System: Windows 11 Professional1 router (TP-Link Archer C1200)
   * Total Estimated Cost: $12,000
2. Multi-function Printer/Fax:
   * Model: 1 Brother MFC-L2710DW
   * Functions: Print, Scan, Copy, Fax
   * Connectivity: Wireless, Ethernet, and USB
   * Estimated Cost: $350
3. Telephone System:
   * Model: 15 Panasonic KX-TGF352N Corded/Cordless 2 Handset Landline Telephone
   * Features: Answering machine, Caller ID, Call Block, Night Mode
   * Handsets: 2 Cordless Handsets with base unit and charger
   * Total Estimated Cost: $1500 total.
4. TP-Link Archer C1200:
   * Supports 802.11ac, the next generation of Wi-Fi, and is backward compatible with 802.11n
   * Offers combined wireless speeds of up to 1200Mbps, with 300Mbps over the 2.4GHz band and 867Mbps over the 5GHz band
   * Estimated Cost: $100

**Software:**

1. Operating System:
   * Product: Windows 11 Professional (included with Dell OptiPlex 3080 Micro)
2. Office Productivity Software:
   * Product: Microsoft Office 365 Business Standard
   * Includes: Word, Excel, PowerPoint, Outlook, OneDrive, Teams, and more
   * Subscription Model: Annual subscription
   * Estimated Cost per User/Year: $150
   * Total for 15 Users/Year: $2,250
3. Security Software:
   * Product: Windows Defender Antivirus
   * Features: Comprehensive, real-time protection against software threats like viruses, malware, and spyware across email, apps, the cloud, and the web. Windows Defender also includes ransomware protection with controlled folder access, network firewall, and internet protection.
   * Operating System Requirement: Built into Windows 11 Professional (included with Dell OptiPlex 3080 Micro)
   * Cost: $0 (No additional cost as it is integrated into the Windows 11 Professional operating system):

Data: Critical business data, including client information, patient health information (PHI), financial records, and employee details.

Network Infrastructure: A simple LAN setup without advanced networking equipment like switches or firewalls.

## Identify Threats:

**Appendix F and G** will show the different entry points of attackers in the system.

* Phishing Attacks: The risk of employees inadvertently divulging sensitive information through deceptive emails. Employees also being in risk through methods such as smishing, vishing, or quishing.
* Malware and Ransomware: Potential infiltration of the network through malicious software, leading to data theft or encryption.
* Unsecured Network Access: Lack of secure Wi-Fi and VPN connections exposes the network to unauthorized access.
* Physical Security Breaches: The possibility of unauthorized physical access to the premises, leading to theft or damage of IT assets.
* Data Breach: The risk of sensitive client and company data being accessed or stolen due to inadequate security measures. The loss of PHI will lead to heavy fines.
* Natural Disasters: Potential damage or loss of IT assets and data due to environmental threats like floods or fires.

## Document Existing Controls:

Data Access Controls: Currently there are no restrictions on data access.

Basic Antivirus: A entry level of protection against viruses and malware. Free software that comes with the operating system.

Password Policies: General password policies without enforcement of complexity or regular updates. No password managers in use for shared credentials.

Physical Security Measures: Standard locking mechanisms for premises without advanced security systems. Locked physical location but no cameras to monitor the area.

## Identify Improvements:

Enhanced Security Software Implementation: Recognizing the advanced form of modern cyber threats, we recommend the deployment of advanced security solutions. Next-generation firewalls, such as the Fortinet FortiGate series, offer a wide variety of network protection, including intrusion prevention, web filtering, and secure VPN capabilities for remote access. Endpoint protection platforms (EPPs) should also be introduced to safeguard individual devices against malware, ransomware, and other attacks, with solutions like CrowdStrike Falcon or Sophos Intercept X providing state-of-the-art defense mechanisms.

Advanced Network Infrastructure Upgrades: The network's foundation needs to be fortified with enterprise-grade hardware capable of supporting enhanced security features and managing complex network traffic efficiently. The current residential grade hardware will need to be upgraded to manage switches like the Cisco Catalyst 2960-X Series which will enable better segmentation of network traffic, using VLANs to isolate sensitive data and systems. Secure wireless access points, such as the Aruba Instant On AP22, should be installed to provide encrypted Wi-Fi access, enhancing security without compromising user convenience.

Data Encryption and Comprehensive Backup Solutions: To protect sensitive information both in transit and at rest, implementing robust encryption protocols is critical. Tools such as BitLocker for disk encryption and SSL/TLS for data in transit can significantly reduce the risk of data breaches. Alongside encryption, a comprehensive backup strategy involving regular, encrypted backups stored both on-site and off-site will ensure data integrity and availability, even in the event of a disaster.

User Training and Awareness Programs: Human error remains one of the largest security vulnerabilities. Developing an ongoing cybersecurity awareness program will educate employees on the importance of security practices, such as recognizing phishing attempts, following password policies, and reporting suspicious activities. Regular training sessions, newsletters, simulated phishing, and security drills can cultivate a culture of security mindfulness across the organization.

Physical and Network Access Control Measures: To prevent unauthorized access to physical and digital assets, implementing stringent access controls is essential. Advanced physical security measures, including surveillance cameras and electronic access control systems, will monitor and restrict entry to sensitive areas. On the network side, techniques such as VPNs for secure remote access, and MAC address filtering on the wireless network, will ensure that only authorized devices can connect to the network, thereby reducing the risk of intrusion.

Policy and Compliance Framework Development: Establishing a comprehensive information security policy, underpinned by detailed Acceptable Use Policies (AUPs), is fundamental to maintaining a secure environment. These policies should define clear guidelines on the use of organizational resources, data handling, and security protocols. Regular audits and compliance checks will ensure adherence to these policies, while also keeping the organization aligned with industry standards and regulations.

# **Target Network**

## Recommended Physical Network:

The proposed physical network upgrade aims to enhance security, efficiency, and scalability. Each recommended hardware component is selected based on performance, cost-effectiveness, and compatibility with the current infrastructure. Please see **Appendix H.**

1. Server: Dell PowerEdge T340 Tower Server
   * Specs: Intel Xeon E-2224 3.4GHz, 16GB RAM, 2x1TB SATA HDD
   * Cost: $1,200
   * Purpose: Hosts centralized file, application services, and Active Directory for user management.
2. Network Switch: Cisco SG250-26 Smart Switch
   * Specs: 26 Port Gigabit Smart Switch, Layer 3 routing capability
   * Cost: $300
   * Purpose: Facilitates connectivity and network segmentation for enhanced security and performance.
3. Firewall: Fortinet FortiGate 60F
   * Specs: Next-Generation Firewall (NGFW) capabilities, VPN support, Integrated SD-WAN
   * Cost: $700
   * Purpose: Provides advanced threat protection, web filtering, and secure remote access.
4. Wireless Access Points: Ubiquiti UniFi AP-AC Pro
   * Specs: Dual-band, 3x3 MIMO technology, 802.11ac
   * Cost: $150 each (x3 = $450)
   * Purpose: Ensures comprehensive Wi-Fi coverage with secure and scalable wireless access.
5. UPS (Uninterruptible Power Supply): APC Smart-UPS 1500VA
   * Specs: 1500VA / 1000W, battery backup and surge protector
   * Cost: $500
   * Purpose: Provides power backup and protection for critical network components

## Recommended Logic Network:

The logical network design segments are accessed for various user groups, incorporating the latest security protocols and network management practices. Please see **Appendix K.**

**Core Network Infrastructure:**

* Firewall: Fortinet FortiGate Next-Generation Firewall will serve as the network's primary defense mechanism, offering advanced threat protection, VPN access, and traffic filtering. Estimated cost: $1,500.
* Switches: Cisco Catalyst 2960-X Series Switches will provide network segmentation capabilities through VLANs, enhancing security and network performance. Estimated cost: $850.
* Wireless Access Points: Ubiquiti UniFi AP-AC Pro devices will offer secure and reliable Wi-Fi coverage throughout the premises, supporting both 2.4 GHz and 5 GHz bands. Estimated cost: $450 for several units.

**Security and Access Control:**

* VPN Solutions: For remote access, a VPN solution will be implemented, using FortiGate's integrated VPN capabilities to ensure secure connections for remote workers. Included in the firewall cost.
* Two-Factor Authentication: Duo Security will provide an extra layer of security for accessing critical systems, ensuring that only authorized users can gain access. Estimated cost: $3 per user/month.

**VLANs:**

The new VLAN setup incorporates the above hardware, segmenting the network into VLANs for security and performance optimization. Key components include:

* VLAN 1: Management - Contains network management and server equipment.
* VLAN 2: Employee Access - Secured access for internal employees, containing workstations and printers.
* VLAN 3: Guest Access - Isolated from the internal network, provides internet access for guests.

Firewall rules and inter-VLAN routing managed by the FortiGate 60F ensure secure and efficient data flow, while the Ubiquiti access points support seamless wireless connectivity across the premises. There is no additional costs as this leverages the hardware purchased for overall improvement.

**Network Services:**

* DHCP & DNS Services: Windows Server 2019 will be configured to handle DHCP and DNS roles, ensuring efficient network address assignment and name resolution. Estimated cost for server license: $972.

## Gap Analysis:

The current network lacks adequate security measures, centralized data management, and fails to meet performance needs for current and future applications. Upgrading hardware and implementing a structured network design address these gaps by introducing robust security controls, efficient data management, and scalable infrastructure.

## SWOT Analysis:

Please see **Appendix J.**

* Strengths: Reliable hardware choices, enhanced security posture, improved network performance.
* Weaknesses: Initial cost of implementation, training needs for staff on new equipment.
* Opportunities: Future scalability, improved data protection, and operational efficiency.
* Threats: Potential cybersecurity threats during migration, ongoing maintenance costs.

## Product Recommendations:

Please see **Appendix I** for the cost table.

1. Issue: Outdated Network Security Measures
   * Proposed Solution: Upgrade to a Fortinet FortiGate Next-Generation Firewall for advanced threat protection, integrated VPN capabilities for secure remote access, and improved network performance management.
   * Estimated cost: $1,500
2. Issue: Inefficient Network Performance and Management
   * Proposed Solution: Implement Cisco Catalyst 2960-X Series Switches for enhanced network segmentation, efficiency, and management, supporting VLANs for secure and organized network traffic flow.
   * Estimated cost: $4,000 (for multiple units as needed)
3. Issue: Limited Wireless Coverage and Security
   * Proposed Solution: Deploy Aruba Instant On AP22 Wi-Fi access points to provide secure, reliable, and extensive wireless coverage throughout the facility, supporting both 2.4 GHz and 5 GHz bands.
   * Estimated cost: $1,200 (for several units to ensure complete coverage)

# **Migration Overview**

The migration to Inomancy Health Care’s new network infrastructure is a comprehensive project designed to enhance security, efficiency, and scalability. This multi-phase approach ensures a seamless transition, minimizes downtime, and addresses the organization's current and future needs.

1. Phase 1 - Planning and Procurement
   * Objective: Lay the groundwork for the migration by establishing a detailed project plan and procuring necessary hardware.
   * Actions:
     + Develop a detailed project timeline, assigning roles and responsibilities to the IT team.
     + Order hardware, including the Dell PowerEdge T340 server, Cisco SG250-26 switch, Fortinet FortiGate 60F firewall, and Ubiquiti UniFi AP-AC Pro access points.
     + Perform a comprehensive backup of all existing data and configurations.
   * Estimated Cost: $6,526
2. Phase 2 - Infrastructure Setup
   * Objective: Establish the foundational network infrastructure for enhanced security and performance.
   * Actions:
     + Install and configure the Dell PowerEdge T340 server to host network services, including file storage, Active Directory, DHCP, and DNS.
     + Set up the Cisco SG250-26 switch, integrating VLAN segmentation for traffic management and security.
     + Deploy the Fortinet FortiGate 60F firewall to enforce robust network perimeter security and to facilitate VPN access for secure remote connections.
   * Estimated Duration: 2-3 weeks.
3. Phase 3 - Network Services Configuration
   * Objective: Configure critical network services and security features to support organizational operations and secure data handling.
   * Actions:
     + Implement VLAN segmentation on the Cisco switch to separate network traffic (e.g., administrative, clinical, guest) enhancing security and performance.
     + Configure DHCP and DNS services on the Dell server for efficient network management.
     + Establish Active Directory for centralized user and device management, improving security and operational efficiency.
     + Set up firewall rules and VPN configurations on the Fortinet firewall, ensuring secure remote access.
   * Estimated Duration: 1-2 weeks.
4. Phase 4 - Wireless Network Deployment
   * Objective: Expand network accessibility while maintaining security through a robust wireless network.
   * Actions:
     + Install Ubiquiti UniFi AP-AC Pro access points to provide comprehensive wireless coverage throughout the facility.
     + Configure separate SSIDs for guest and employee access, applying appropriate security measures and access controls.
   * Estimated Duration: 1 week.
5. Phase 5 - Testing and Optimization
   * Objective: Ensure the new network meets all operational requirements and optimizes performance.
   * Actions:
     + Conduct extensive testing of network functionalities, including connectivity, bandwidth, security measures, and failover capabilities.
     + Gather feedback from end-users to identify any performance issues or bottlenecks.
     + Optimize network configurations based on testing results and feedback to ensure peak performance and user satisfaction.
   * Estimated Duration: 2 weeks.
6. Phase 6 - Training and Documentation
   * Objective: Equip staff with the knowledge to effectively use the new network infrastructure and maintain security practices.
   * Actions:
     + Provide training sessions on new network features, security protocols, and best practices for cybersecurity.
     + Create comprehensive documentation of network configurations, policies, and procedures to facilitate ongoing maintenance and troubleshooting.
   * Estimated Duration: 1 week.
7. Phase 7 - Go Live and Monitoring
   * Objective: Officially transition to the new network infrastructure and implement monitoring for continuous improvement.
   * Actions:
     + Transition all operations to the new network, closely monitoring system performance and security alerts.
     + Utilize network monitoring tools to track performance metrics, identifying areas for future enhancements or adjustments.
   * Ongoing Post-Implementation

# **Conclusion**

Transitioning to the new network infrastructure represents a significant leap forward for Inomancy Health Care, promising enhanced security, improved performance, and greater scalability. This carefully planned migration minimizes operational disruptions and lays a solid foundation for future technological advancements, ensuring the organization remains at the forefront of healthcare IT.

**Top of Form**

# **Appendix**

## Appendix A - IT Governance Structure

## Appendix B - Enterprise Architecture

A diagram of a computer network

Description automatically generated

## Appendix C – Risk Assessment with Original Setup

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Factor | Description | Impact Level | Likelihood |
| Lack of VPN | **The network does not support Virtual Private Networks (VPNs), making remote work less secure.** | **High** | **Medium** |
| Minimal Access Controls | **Without sophisticated access controls, all users have similar network access levels, increasing the risk of unauthorized data access.** | **High** | **High** |
| No Network Switch | **The absence of a network switch limits the ability to segment traffic, leading to potential performance bottlenecks and security risks.** | **Medium** | **High** |
| Unrestricted File Access | **The lack of file restrictions means sensitive information may be accessible to all users, increasing the risk of data breaches.** | **High** | **Medium** |
| Basic Antivirus Protection | **Reliance on Windows Defender without additional antivirus measures may not fully protect against advanced threats, though it provides basic security.** | **Medium** | **Medium** |
| Limited Hardware Security | **The simple modem/router setup and absence of specialized network hardware suggest limited security capabilities, increasing vulnerability to cyber-attacks.** | **High** | **High** |
| No Specialized Network Hardware | **The lack of VOIP phones or advanced networking devices suggests a basic setup that may not support sophisticated security or performance features.** | **Medium** | **Low** |
| Dependence on Single Internet Connection | **Relying on a single modem and router for internet access poses a risk of complete network failure in the event of device malfunction or service interruption.** | **High** | **Medium** |

## Appendix D – Risk Assessment with Recommended Setup

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Factor | Description of Mitigation | Impact Level After Upgrade | Likelihood After Upgrade |
| Network Security Vulnerabilities | Upgrading to a Fortinet FortiGate Next-Generation Firewall significantly enhances threat protection, including advanced web filtering and intrusion prevention. | Low | Low |
| Network Performance Issues | Implementing Cisco Catalyst 2960-X Series Switches improves network efficiency and supports VLANs for organized traffic flow, reducing congestion and bottlenecks. | Low | Low |
| Wireless Security and Coverage | Deploying Ubiquiti UniFi AP-AC Pro access points ensures comprehensive, secure Wi-Fi coverage, supporting seamless access control and encrypted connections. | Low | Low |
| Power Outage Vulnerability | The addition of APC Smart-UPS 1500VA provides reliable battery backup to critical network components, reducing the risk of downtime due to power failures. | Low | Low |
| Remote Access Vulnerabilities | Integrated VPN capabilities in the Fortinet FortiGate firewall, coupled with Duo Security's two-factor authentication, offer secure remote access, minimizing the risk of unauthorized entry. | Low | Low |
| Lack of Network Segmentation | Cisco SG250-26 Smart Switch facilitates effective network segmentation, enhancing security by isolating sensitive data and reducing cross-network threats. | Low | Low |
| Data Loss and Recovery Concerns | Centralizing services on the Dell PowerEdge T340 Tower Server, along with implementing a robust backup strategy, improves data integrity and disaster recovery capabilities. | Low | Low |
| Inadequate Access Control | Active Directory services on the new server enhance access control, allowing for granular user permissions and reducing the risk of unauthorized data access. | Low | Low |

## Appendix E - Current Infrastructure Cost

|  |  |  |
| --- | --- | --- |
| Hardware/Sofware Model: | Quantity: | Cost: |
| Dell OptiPlex 3080 Micro | **15** | **$12,000** |
| TP-Link Archer C1200 | **1** | **$100** |
| Brother MFC-L2710DW | **1** | **$350** |
| Panasonic KX-TGF352N | **15** | **$1,500** |
| Office Productivity Suite | **15/annual** | **$2,250** |
|  |  |  |
| Total Cost: | **$16,200** |  |

## Appendix F – Identify Threats

**Threat Scenario: Phishing Attacks**

|  |  |
| --- | --- |
| **Criteria** | **Details** |
| **Threat** | **Phishing Attacks** |
| **Description** | **Malicious actors trick employees into revealing sensitive data by masquerading as trustworthy entities through emails or fake websites.** |
| **Likelihood** | **Medium** |
| **Vulnerability** | **Employee susceptibility to social engineering tactics due to lack of awareness.** |
| **Impact** | **High** |
| **Mitigation** | **Implement regular security awareness training focusing on recognizing phishing tactics. Utilize email security solutions that filter out phishing emails.** |
| **Impact Area** | **Financial, Reputation** |
| **Risk Score** | **6/10 (Medium likelihood x high impact)** |
| **Adequacy of Existing Controls** | **Fortinet FortiGate 60F provides email filtering capabilities. Ongoing employee training programs are in place to combat phishing.** |

## Appendix G – Identify Threats

**Threat Scenario: Ransomware Infection**

|  |  |
| --- | --- |
| **Criteria** | **Details** |
| **Threat** | **Ransomware Infection** |
| **Description** | **Malware encrypts files, demanding ransom for decryption. It often infiltrates through malicious downloads or email attachments.** |
| **Likelihood** | **Medium** |
| **Vulnerability** | **Insufficient endpoint protection and awareness regarding malicious attachments.** |
| **Impact** | **High** |
| **Mitigation** | **Use Windows Defender for endpoint protection with real-time scanning. Conduct data backups regularly. Educate employees on safe browsing and email habits.** |
| **Impact Area** | **Operational, Financial** |
| **Risk Score** | **6/10 (Medium likelihood x High impact)** |
| **Adequacy of Existing Controls** | **Enhanced endpoint security with Windows Defender and backup solutions. Ongoing cybersecurity awareness training.** |

## Appendix H – Recommended Physical Network

**A diagram of a computer network

Description automatically generated**

## Appendix I – Target Infrastructure Cost

|  |  |  |
| --- | --- | --- |
| Hardware/Software Model: | Quantity: | Cost: |
| Server: Dell PowerEdge T340 Tower Server | 1 | $1,200 |
| Network Switch: Cisco SG250-26 Smart Switch | 1 | $300 |
| Firewall: Fortinet FortiGate 60F | 1 | $700 |
| Cisco Catalyst 2960-X Series Switch | 1 | $850 |
| Firewall: Fortinet FortiGate Next-Generation Firewall Software | 1/annual | $1,500 |
| Wireless Access Points: Ubiquiti UniFi AP-AC Pro | 3 | $450 |
| UPS (Uninterruptible Power Supply): APC Smart-UPS 1500VA | 1 | $500 |
| Two-factor Authentication: Duo | 18/annual | $54 |
| DHCP & DNS Services: Windows Server 2019 | 1/annual | $972 |
|  |  |  |
| Total Cost: | $6,526 |  |

## Appendix J – SWOT Analysis

**A diagram of a project

Description automatically generated with medium confidence**

## Appendix K – Recommended Logical Network

**A diagram of a computer network

Description automatically generated**

## Appendix L – Current Physical Network

**A diagram of a room with people sitting at tables

Description automatically generated**

## Appendix M – Current Logical Network

A diagram of a computer network

Description automatically generated

## Appendix N – Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Network Security Measures Gap Analysis** | | | | | |
| **Business Unit:** | Information Technology | | | | |
| **Gap Analysis:** | There are virtually no restrictions in place on the network. | | | | |
| **Recommendations:** | Implement VPN, add access controls, reinforce the existing antivirus, and segment the network | | | | |
| **Gap Analysis Metrics:** | **Met** | **Somewhat Met** | **Not Met** | **Strengths** | **Weaknesses** |
| Antivirus |  | **X** |  | There is a basic antivirus in place that will warn the user of suspicious software but will not prevent the installation. | The current antivirus comes free with the operating system and will not do a great job in removing malware once installed. |
| VPN |  |  | **X** |  | All the Ips are on a public network allowing anyone to access the systems even without valid credentials. |
| Firewall |  | **X** |  | Currently using Windows Defender to block off unwanted incoming traffic. | More layers of security can be added to further strengthen the free software that is in use. |
| Network Segmentation |  |  | **X** |  | Without network segmentation, an attacker would have full access to any sensitive information because it is not segmented and restricted. |

## Appendix N – Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Centralized Data Management Gap Analysis** | | | | | |
| **Business Unit:** | Information Technology | | | | |
| **Gap Analysis:** | Data access controls are not set in place. | | | | |
| **Recommendations:** | Need to set access controls, a recovery plan, and set policies to enforce a healthy standard by blocking remote access vulnerabilities. | | | | |
| **Gap Analysis Metrics:** | **Met** | **Somewhat Met** | **Not Met** | **Strengths** | **Weaknesses** |
| Access Controls |  |  | **X** |  | All of the employees have the same level of access. Phished credentials would have admin level access to data. |
| Data Loss and Recovery |  | **X** |  | Some of the data is stored in OneDrive. | There is not a central place that all the data is stored. There are no policies in place to manage the data. |
| Remote Access Vulnerabilities |  |  | **X** |  | Data can be accessed while working remotely on personal devices that are not managed by the business. |