Bachelors Degree Program

TAYLOR' S UNIVERSITY
Wisdom • Integrity • Excellence

Module Code : ITS67304 (February 2024)

Module Name : Wireless Networks and Security

Assignment No./Title	**Group Assignment (20%)**
Course Tutor/Lecturer	Mr. Sham Shul Shukri Mat
Submission Date	10th Mar 2024

Student Name, ID and Signature

1. Nicki Gan Wei Fern, 0356830, Hickian
2. Ooi Khe Foh, 0356581, Brandon
3. Nirmal Kavindu Athukorale, 0358879, Kavi
4. Tapas Mohamed Amir, 0361429, Ragad

Declaration *(need to be signed by students. Otherwise, the assessment will not be evaluated)*

Certify that this assignment is entirely my own work, except where I have given fully documented references to the work of others, and that the material contained in this assignment has not previously been submitted for assessment in any other formal course of study.

Marks/Grade:	**Evaluated by:**

Evaluator's Comments:

The objective of this special assessment is to enable the students to:
Describe and develop fundamental principles of information security (MLO1).

Table of Contents

1.0 Purpose of Design

MHC, a medium-sized media and advertising company with approximately 25 employees and 20 PCs, recognizes the critical need to overhaul its current computer and network infrastructure. This strategic move is motivated by a desire to embrace the e-business era, providing services via the Web (Internet) for their customers and intranet for their staff. MHC's current outdated network and computer infrastructure is based on wired connections, computers with outdated operating systems, and network infrastructure with little to no security in place. The purpose of this new network design is to propose an efficient network layout that will improve operational efficiency and security procedures, enable future expansions, and bring MHC computer and network infrastructure to the next level. An important goal of MHC is to achieve cost-effectiveness with consideration for the distribution of resources and improvements in technology.

Segmentation plays a crucial role in the design's purpose, as MHC plans to segment the internal network into five distinct segments. This is done to facilitate streamlined operations, offer upgraded security by restricting access to sensitive data, and optimizes resource allocation for each department. The decision to switch to wireless networking comes from the need to create a more dynamic workspace that fosters a more flexible work environment where employees can work from different locations in the company improving cooperation and innovation. While wireless solutions cater to end-user devices, critical components like ISP connections and the backbone remain wired for stability and enhanced security. This approach provides the necessary flexibility for staff mobility without compromising the stability of essential network components. Simultaneously, the universal upgrading of operating systems aligns with the goal of decreasing vulnerabilities associated with outdated software while also ensuring interoperability with the latest technologies. The implementation of ISO/IEC 27001 and related security standards shows a commitment to protecting client data and intellectual property, going beyond regular compliance and regulations, and positioning MHC as a trusted protector in the industry.

This is a strategic plan to satisfy unique operational needs within each unit and support efficient processes within each department. The adoption of open-source web hosting solutions in the IT and online sectors exemplifies a forward-thinking approach that leverages new technologies to improve service delivery and operational efficiency. This network design specification is an important element in not only upgrading existing infrastructure but also strategically placing the company for long-term growth and competitiveness. The network design prepares MHC to tackle the changing, evolving business environment and innovations by addressing several issues, including cost-effectiveness, improved security, and technological adaptability.

2.0 Conceptual Design of Network Layout

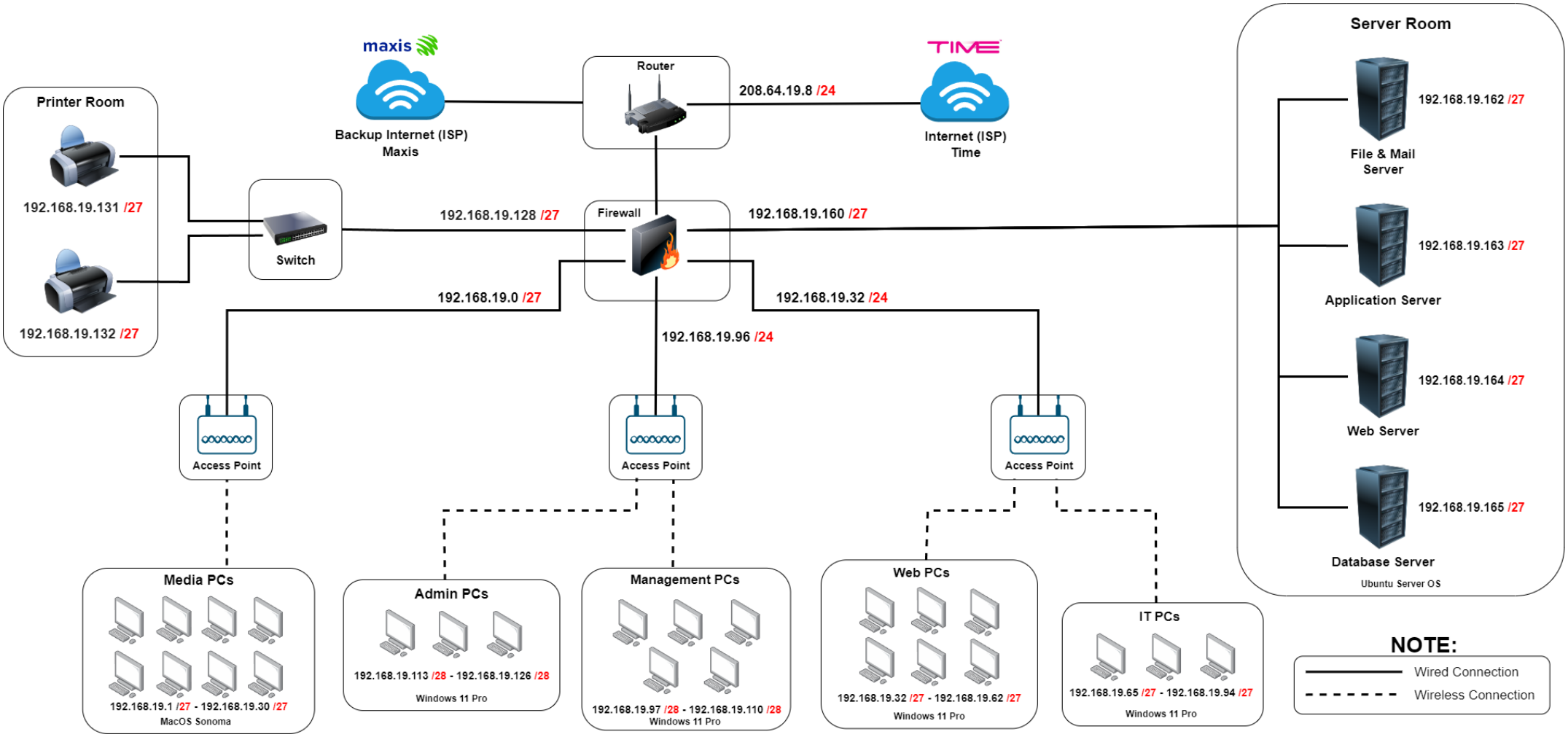

Diagram link: https://app.diagrams.net/#G14NWOgWiug5uk4qexT6U3RRHDkz6T-ErO#%7B%22pageId%22%3A%225LNXIwAaSpPEIEEEKctR%22%7D

Explanation & Justification of the Network Diagram

We have decided the most suitable network diagram for Munkirk Hayern Corporation (MHC) is one that is cost-efficient and able to transmit data as quickly as possible. There are a total of 25 PCs which are separated into 5 departments. Due to cost-efficiency demands within the company, three access points are allocated for the five departments. However, only one department fully utilizes them, namely the media department. This is because they require a strong internet connection for various purposes such as file sharing, content streaming, research, and trend monitoring, among others. The other four departments will share the two access points. The access points will be connected to the firewall and router to receive the internet. Furthermore, there are also two printers which are connected to a switch. The switch will be connected to the firewall and router so that it can connect with those PCs.

We will have one central router (provided by the ISP) which is connected to a **firewall** for the entire network; connecting the 4 servers in the server room, the three access points that connect the five departments, and the switch that connects the two printers. We have strategically placed the firewall between MHC's internal network and the external network to ensure that unauthorized users don't interfere with the network as MHC provides Web services to the public.

We opted to go for 4 **servers**; namely the File and Mail server, Application, Web, and Database. The file and mail server are used to send and receive mail as well as host all kinds of files. The application server is used to enable the interaction between the end user and the company server side. The web server manages traffic, both requests to and responses from the client system; It also focuses on holding the website data and protecting it. The database server is for MHC's information storage and management needs. It stores and manages databases on the servers, such as user information. Each of these servers is given a fixed IP address in the network taken from the 'Extra' range of IP address ranges; separate from the department's subnet IP address ranges. The servers are accessible by the departments depending on their operations and access will be granted according to the firewall and router rules.

Our two **printers**, meant to be shared between the Media, Admin, and Management departments are connected by a switch, their IP addresses are just like the servers; taken from the 'Extra' range of IP addresses. Connecting the printers to the network, we used a device known as a switch which is connected to the firewall. Departments that are allowed access to the printers will be determined by the router, accessing through the fixed IP addresses of the printers.

The firewall connects to 3 **wireless access points**. We opted for three instead of an access point per department to reduce costs and make the networking more efficient. The Management and Admin departments are meant to share an access point and so do the Web and IT departments since we felt that the departments that share an access point would be required to access a lot of the same data. The Media department has its own access point due to the assumption that this department is the busiest and requires high network traffic. With MHC being a media company, we assume that the media department will have the most information flowing through it, hence, it has an access point to itself and more computers than any other department. This is to ensure the workflow of the media is more efficient and there will be no disruptions to Media's important work. The IP addresses of the wireless access points correspond to the departments they connect to.

The servers and printers can only be accessed by selected departments, the policies set on the firewall ensure that departments that do not need access to certain printers and servers would not have access. Additionally, the company is given a backup ISP to prepare for any server downtime caused by the main ISP and a failover connection with the main ISP will not affect the business and its clients. Apart from the backbone, servers access and printers, and connection to ISP, the network is mostly wirelessly based to improve flexibility and mobility of the connections and departments are allow to move around with ease.

Assuming that MHC is a Malaysian-based company, we propose that the main ISP for them should be services provided by Time Internet, voted one of the best internet service providers in the country, with excellent speeds and decent customer support. The backup ISP should be just as capable, hence why we have opted to go for Maxis, extremely common in Malaysia with great speeds and support. Maxis and Time Internet are the two best choices in Malaysia. According to (Wong, 2023), Time average speed is 108.38Mbps and Maxis' speed is 92.61Mbps, these two brands are in the top three rank in Malaysia. Furthermore, the Time Internet consistency of speed is 88.2, followed by Maxis is 86.3. In our opinion, these two ISPs are the best choice MHC can get in Malaysia.

To add on, Time and Maxis have extensive coverage across Malaysia, so it can ensure that MHC's office and facilities can access high-speed internet services across Malaysia. Maxis and Time Internet also offer technical support teams that operate 24/7, so that if MHC has any connection issues or technical challenges, they can always call their hotline and solve their issue immediately by the ISP (Maxis, n.d) (Time, n.d).

Limitations of Network Design

1. Failure of either the second or third wireless access point would mean that 2 departments will go offline, either the Web or IT of the management and Admin departments.
2. The firewall being the central connection point would mean that if it were to fail the entire network would suffer and the whole company would go offline.
3. All the departments are wirelessly connected, despite helping save costs on wiring and maintenance, it is more unreliable and will produce slower speeds compared to a wired connection.

Besides, in the proposed network diagram, the IDF (Intermediate Distribution Frames) and MDF (Main Distribution Frame) play an important role in managing network connectivity and distributions, assuming that MHC's office consists more than one floor. The IDF has three access points and one switch which helps the connectivity in the building of MHC, it helps keep the network strong and prevent connectivity problems. On the other hand, the MDF is where all the connectivity comes together as one. MDF has the most important equipment, which are the router and the servers. The MDF makes sure that data can run smoothly across different parts of the network. With IDF and MDF working together MHC does not have to be worried about connection and reliability of their internet across their offices and facilities. Overall, the network was designed to achieve high efficiency and security, whilst being cost-effective as proven in our diagram shown above.

3.1 Proposed Operating System for MHC's Operations

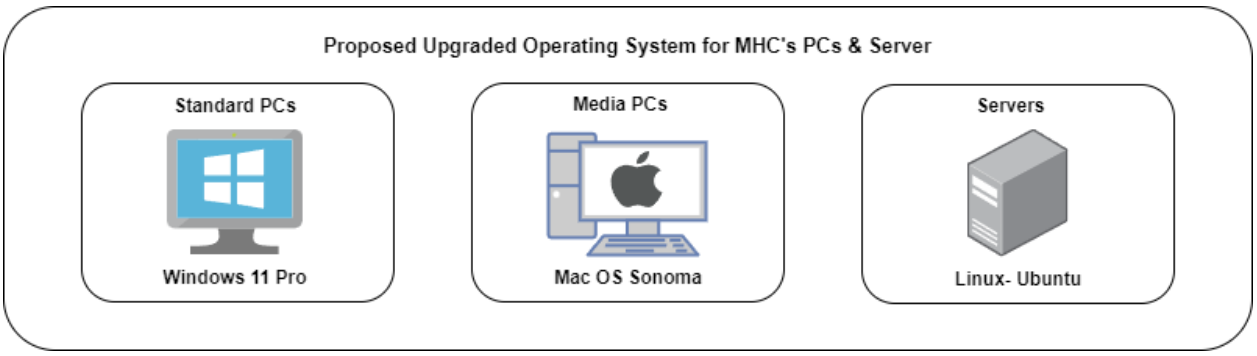

Figure 2.0 - Summary of the proposed Operating System upgrades

Operating System for PCs

For all employees of the Admin, Management, Web, and IT Department, we propose to upgrade the operating system of their personal computers to **Windows 11 Pro**; compared to the previously used Windows 10 Home. Upgrading the company's operation system is important because newer versions often receive more consistent security updates and patches. Upgrading your OS will ensure all of MHC's PCs are protected against the latest security threats and maintain a secure computer work environment. A newer operating system often ensures optimization that will lead to improved overall system performance. Upgrading from Windows 10 to Windows 11 enables better performance as it prioritizes foreground apps and has fewer default background processes consuming resources. If employees of MHC are interested in using the latest applications, upgrading the operating system is necessary to allow new applications to run smoothly. (Windows 11 et al., n.d.)

The main reason for a business such as MHC to upgrade to Windows 11 Pro is due to its security features. Both Windows 11 Home and Windows Pro may have basic device encryption, however, BitLocker encryption is only exclusively supported by the Pro versions. It protects sensitive files with specific drive encryption and mitigates the risk of data breaches (Microsoft, 2023) Besides that, Windows 11 Pro comes with Windows Information Protection (WIP), a data loss prevention tool used to prevent data leakage within the company. MHC can use this feature to prevent personnel from forwarding content to external parties while allowing the IT department to delete business data remotely without affecting personal data if a PC is ever lost or stolen. (xda-developers, 2024)

The Home versions may possess great advanced security measures such as Device Guard and Secure Boot which adds an extra layer of defense against malware while securing critical systems

for editing and production. However, Domain Join, which is only available in Pro versions of Windows, simplifies user account management, enforces consistent security policies across devices, and saves the IT Department large amounts of time (Lenovo, 2023). With Domain Join, admin and management tasks would be streamlined with centralized control, allowing efficient management of user accounts and policies, and freeing up time for strategic planning and decision-making. A trust relationship is built between the computer and the domain controller. The domain controller is used to authenticate users, manage policies, and grant access to network resources. Once the computer joins a domain, it becomes a member of the domain and can take advantage of the centralized management and security features provided by the domain infrastructure.

Another beneficial feature of the Windows 11 Pro is the Remote Desktop feature which enables efficient troubleshooting and management, which is particularly useful for remote teams of off-site employees and freelancers of MHC. Assuming that MHC will have remote IT employees who work from home, Remote Desktop is a beneficial feature used for efficient troubleshooting where IT professionals can diagnose and resolve issues on remote PCs quickly, reducing MHC's cost and downtime. It also helps to reduce MHC's cost, employees are allowed to use Remote Desktop to work remotely, eliminating the need for physical office space and hardware. (Jonson, 2023)

Additionally, Windows 11 Pro simplifies device management with Group Policy, streamlining the configuration of software updates, security protocols, and user permissions. Group Policy is used to ensure your central IT infrastructure and information are configured securely. They are very effective in addressing the security gaps and particularly useful when implementing a policy of least privilege. The Group Policy drastically improves security by disabling outdated protocols and preventing unauthorized users from making changes. (Kisi Access Solutions, n.d.) MHC's Management department would achieve improved compliance by enforcing consistent security policies through Group Policy, used to ensure adherence to industry regulations. Cost optimization is facilitated by Hyper-V, a virtualization tool, which allows the operation of multiple virtual machine applications on a single machine. This could potentially reduce the hardware costs of MHC as Hyper-V allows for the installation of different operating systems like Linux without purchasing a different machine while doing it all risk-free.

Windows 11 Pro offers valuable benefits in terms of security, management, and functionality compared to Windows 10 Home and even Windows 11 Home. Despite costing $60 more than Windows 11 Home, it would eventually prove to be worth the extra price in terms of security and production for MHC.

For the media PCs, we opted to go for the latest version of the macOS, **macOS Sonoma**, also known as macOS 14 brought substantial improvements in performance through features like Metal 3, enhancing graphics performance and efficiency. This was especially advantageous for creative professionals involved in resource-intensive tasks like video editing and 3D rendering, quite fitting for a media company. The update also prioritized faster app launching, resulting in quicker startup times and reduced memory usage for a more responsive user experience (apple.com, 2023).

Security and privacy enhancements were a key focus, with the implementation of sandboxing to restrict application access to system resources, significantly improving overall system security. Safari received updates in tracking prevention and website sign-in features, reinforcing user protection against online threats. The macOS Sonoma represented a substantial advancement over the previously used Mac OSX v10.11, offering improved performance, innovative features, and heightened security and privacy measures. The upgrade provided an opportunity to enhance user experience and workflow efficiency, particularly beneficial for demanding tasks on Mac devices (macworld.com, 2024).

The macOS Sonoma brings valuable upgrades to MHC’s media department. The improved graphics performance, thanks to Metal 2, accelerates video editing and rendering, leading to quicker project completion and increased productivity. The system's enhanced responsiveness, along with features like Dark Mode and Voice Control, caters to media professionals' needs for reduced eye strain and hands-free control. New functionalities contribute to better project organization and collaboration. Security features like sandboxing and Safari's tracking prevention ensure data protection and privacy, crucial for handling confidential information in MHC’s production. Overall, macOS Sonoma has the potential to significantly improve efficiency, productivity, and security in MHC’s media department (theverge.com, 2023).

Some disadvantages that stand for the operating systems though, Windows 11 include the price of upgrading, which will cost the company around $60 more per device, although the company will find its worth over time, there will also be a bit more of a learning curve for the users to get used to a new operating system (makeuseof.com, 2021). Another disadvantage is that the computers will have to use more resources to run the operating system. mac OS Sonoma also carries around this weight, draining more resources but these problems are assumed for a trade off of better overall performance and more up-to-date patches. (digitaltrends, 2023)

Comparison Table between Windows Operating System

	Windows 10 Home	**Windows 11 Home**	**Windows 11 Pro**
Security	Basic security features like Windows Defender antivirus.	Similar to Windows 10 Home with basic security features.	Enhanced security features like BitLocker encryption and Windows Hello.
Performance	Works okay on different types of computers, but it is as fast as Mac OS on Apple devices.	It runs decently, ensuring tasks are done without much delay.	It offers smooth performance, but it is enhanced for business tasks and multitasking.
Software Compatibility	Compatible with a wide range of software available for Windows.	Compatible with a wide range of software available for Windows.	Compatible with a wide range of software available for Windows.
Productivity Tools	Microsoft Office Suite, Microsoft Edge, Windows Mail & Calendar, Onedrive, and Microsoft Teams	Microsoft Office Suite, Microsoft Edge, Windows Mail & Calendar, Onedrive, and Microsoft Teams	Microsoft Office Suite, Microsoft Edge, Windows Mail & Calendar, Onedrive, and Microsoft Teams

Comparison Table between Mac Operating System

	Mac OSX v10.11	**macOS Sonoma**
Security	Built-in Gatekeeper, XProtect, and FileVault.	Built-in Gatekeeper, XProtect, and FileVault.
Performance	Runs smoothly on Mac computers, it is quick & doesn't freeze or slow down much.	Improved latest Apple devices, delivering an enhanced user experience.
Software Compatibility	Compatible with software designed for macOS.	Compatible with software designed for macOS.
Productivity Tools	Pages, Number, and Keyboard, Safari, Mail and Calendar, Icloud, Messages and Facetime	Pages, Number, and Keyboard, Safari, Mail and Calendar, Icloud, Messages and Facetime

Operating System for Servers

For the server, we recommend changing the operating system to Ubuntu Server for Munkirk Hayern Corporation (MHC). It is an upgrade compared to Windows Server 2022 Standard Edition. There are several factors to consider while making this decision. First of all, Ubuntu is free to download compared to Windows Server 2022 Standard Edition, the previous server OS required a license fee (Ubuntu, n.d), this is perfect for MHC's goal of cost efficiency.

Secondly, the security of Ubuntu is almost the same as Windows Server 2022 Standard Edition according to (TrustRadius, n.d). It has great security features and regular updates (Andreja Velimirovic, 2023), MHC can depend on Ubuntu server security and does not have to worry about potential threats.

Thirdly, Ubuntu also offers flexibility and scalability. It is designed to work on different types of hardware, so if MHC's current hardware is not the latest, the Ubuntu server can still perform accordingly. Moreover, Ubuntu can be customized to suit MHC's unique requirements. So that there won't be any staff accessing data that they should not have. If MHC has any problem with Ubuntu, there is a supportive community and experts ready to assist and advise them. (Broadberry, n.d)

In our opinion, Ubuntu Server's OS is a perfect upgrade for MHC. It is cost-efficient, and has a great security system, flexibility, and strong community support. With the Ubuntu server powering its server OS, MHC can focus on moving its business forward without worrying about its security and reliability.

However, Ubuntu Server's OS offers numerous advantages, but there are still a few disadvantages. By changing their current server's OS to Ubuntu, MHC's staff may need to learn new tools and commands, which is time-consuming. Furthermore, according to (Nonis, 2024), Ubuntu is not a good choice for beginners to use, as it might get challenging while using it. Moreover, the packages that are included in Ubuntu are quite large, some of the packages are not even necessary for MHC (Nonis, 2024). Despite these issues, with proper training and support to their staff, MHC can fully utilize Ubuntu Server's OS and gain benefit from it.

4.0 IP Addressing Scheme for MHC

Munkirk Hayern Corporation has five separate departments namely the **Media, Admin, Management, Web, and IT departments**. They have decided to use the Variable Length Subnet Mask (VLSM subnetting) to assign different numbers of IP addresses for each department depending on the number of PCs and devices used in the department. This method helps to increase the usability of subnets as they can be of variable sizes.

We will assign Media, Web, and IT with a larger range of 32 IP Addresses. Admin and Management will be assigned a smaller number of 16 IP Addresses. A few extra ranges of IP Addresses are used for servers, printers, routers, and for future expansion of MHC's departments.

Network Private IP Range for each department:

Department	Subnet Mask	Network Address	Usable Private IP Address Range		Broadcast Address
Media	255.255.255.224	192.168.19.0/27	192.168.19.1	192.168.19.30	192.168.19.31
Web	255.255.255.224	192.168.19.32/27	192.168.19.33	192.168.19.62	192.168.19.63
IT	255.255.255.224	192.168.19.64/27	192.168.19.65	192.168.19.94	192.168.19.95
Management	255.255.255.240	192.168.19.96/28	192.168.19.97	192.168.19.110	192.168.19.111
Admin	255.255.255.240	192.168.19.112/28	192.168.19.113	192.168.19.126	192.168.19.127
Extra	255.255.255.224	192.168.19.128/27	192.168.19.129	192.168.19.158	192.168.19.159
Extra	255.255.255.224	192.168.19.160/27	192.168.19.161	192.168.19.190	192.168.19.191
Extra	255.255.255.224	192.168.19.192/27	192.168.19.193	192.168.19.222	192.168.19.223
Extra	255.255.255.224	192.168.19.224/27	192.168.19.225	192.168.19.254	192.168.19.255

Fixed IP Addresses:

External IP Address for the Web Server = **208.64.19.8 /24**

Internal IP Address for Web Server = **192.168.19.164 /27**

IP Address for Application Server = **192.168.19.163 /27**

IP Address for File & Mail Server = **192.168.19.162 /27**

IP Address for Database Server = **192.168.19.165 /27**

Calculations:

Media Department	1. To find the number of addresses: 2^5 = 32 addresses 2. The number of bits borrowed from the host: 3 3. Calculating the Subnet Mask: 128 + 64 + 32 = 224 IP Range = **192.168.19.0 - 192.168.19.31** Subnet Mask = **255.255.255.224 /27** Usable IP Addresses = **30**
Web Department	1. To find the number of addresses: 2^5 = 32 addresses 2. The number of bits borrowed from the host: 3 3. Calculating the Subnet Mask: 128 + 64 + 32 = 224 IP Range = **192.168.19.32 - 192.168.19.63** Subnet Mask = **255.255.255.224 /27** Usable IP Addresses = **30**
IT Department	1. To find the number of addresses: 2^5 = 32 addresses 2. The number of bits borrowed from the host: 3 3. Calculating the Subnet Mask: 128 + 64 + 32 = 224 IP Range = **192.168.19.64 - 192.168.19.95** Subnet Mask = **255.255.255.224 /27** Usable IP Addresses = **30**
Management Department	1. To find the number of addresses: 2^4 = 16 addresses 2. The number of bits borrowed from the host: 4 3. Calculating the Subnet Mask: 128 + 64 + 32 + 16 IP Range = **192.168.19.96 - 192.168.19.111** Subnet Mask = **255.255.255.240 /28** Usable IP Addresses = **14**
Admin Department	1. To find the number of addresses: 2^4 = 16 addresses 2. The number of bits borrowed from the host: 4 3. Calculating the Subnet Mask: (128 + 64 + 32 + 16) IP Range = **192.168.19.112 - 192.168.19.127** Subnet Mask = **255.255.255.240 /28** Usable IP Addresses = **14**

Explanation and Justification of IP Addressing Scheme:

Segmenting the network by different departments enhances the security of the network and allows for easy management of the network. With dedicated subnets for each department, the departments can only communicate with each other if the router permits it. Each department has its dedicated IP address range, promoting organization, and simplifying troubleshooting of networks. Besides that, we proposed to use Variable Length Subnet Masking (VLSM) for the subnetting process of the 5 different departments as it promotes efficient utilization of IP addresses by allocating different-sized subnets and minimizes IP address wastage. The IP addresses for each department are dynamic in which the DHCP server will automatically assign devices an IP address from the assigned range, eliminating the need for manual configurations. Dynamic IP addressing allows for IP address reuse and scalability of the departments as the number of devices can change dynamically.

In addition, the IP addresses for all MHC servers are assigned a dedicated subnet to facilitate easy management and enhance security by isolating server traffic from general user traffic. The servers and printers have fixed IP addresses to ensure stability and reliability as changing IP addresses can lead to disruption in service and connections. Fixed IP addresses also make it easier to configure and manage security settings for specific devices, enhancing network security.

Weaknesses of the IP Addressing Scheme:

A notable weakness in the proposed IP addressing scheme lies in the allocation of a fixed number of IP addresses for 'Extra' ranges. This could potentially lead to IP address exhaustion if multiple independent services or departments requiring only a few IP addresses are introduced in the future.

Assumption of design in terms of IP Addressing Scheme:

An assumption was made about the future expansion of MHC where the consideration of IP address exhaustion in the long term has been made and a proactive plan will be made for subnet expansion. With VLSM, we can avoid IP address exhaustion temporarily. Furthermore, it is assumed that robust security measures, including firewalls and access controls, will be implemented to mitigate potential risks associated with shared network segments and external servers. This assumption emphasizes the importance of implementing adequate security policies for overall network protection.

5.0 Recommended Information Security Standards

Securing confidential client data and intellectual property is an important matter to Munkirk Bayern Corporation (MHC) in the evolving media world. The emergence and growth of e-business have made a strong information security architecture even more essential. We propose that MHC adopt the ISO/IEC 27001 as a security standard. ISO/IEC 27001: Information Security Management System (ISMS) is a security standard that clearly defines the requirements for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS) and plays an important step in strengthening its information security procedures in the company. The importance of risk management within ISO/IEC 27001 security standards becomes very important, especially considering MHC's role in managing confidential client information such as databases that have client data and information and intellectual property such as copyrights and patents available. Because sensitive data is shared constantly across the company, MHC works in an industry where continuous risk assessments and the creation of efficient security plans are critical.

Furthermore, ISO/IEC 27001 will guarantee that MHC implements the strictest data protection standards in addition to complying with legal and regulatory obligations regarding information security. This certification will serve as a concrete example or proof of MHC's commitment to protecting customer information, which enhances its standing in a sector where customer confidence is crucial. This ensures that our information security practices remain not only effective but also adaptable to the ever-changing landscape of emerging threats. The standard acts as a dynamic playbook, keeping MHC ahead of the industry's evolving challenges. The continuous improvement emphasis of the standard fits in well with MHC's dynamic operations as a media company, guaranteeing that its information security procedures continue to be efficient and flexible in the face of new threats.

At Munkirk Hayern Corporation, the implementation of the ISO/IEC 27001 standard will be advantageous for several departments. This includes the IT division, where the standard guarantees the adaptability and security of IT networks and systems, which line up with the strategic goals of the company. The Web department gains from a tailored approach that enables security measures to be tailored to particular risks in the evolving digital landscape, guaranteeing that cybersecurity plans are in line with web-based business goals. Furthermore, the standard's risk management and legal compliance sections directly address issues the Media Services department faces or might face. The department benefits from the standard's provisions, which ensure adherence to regulatory requirements, given its role in handling sensitive media content.

Other standards like the NIST Cybersecurity Framework and the NIST SP 800-53 are possible standards that MHC might want to consider adopting as well. The NIST SP 800-53 provides a framework of security controls and guidelines that can be tailored to address the unique needs and risks of different organizations, while the NIST Cybersecurity Framework (CSF) is a set of guidelines, best practices, and standards developed by the National Institute of Standards and Technology (NIST) in the United States. It provides a flexible and voluntary framework for organizations to manage and improve their cybersecurity posture. Both are great standards to ensure the highest security protocols are established in MHC, however, adopting a minimum of one standard is enough for MHC.

Conclusion:

In conclusion, MHC's commitment to information security is evident through its strategic adoption of ISO/IEC 27001. These standards and measures collectively address crucial aspects of MHC's information security needs, ranging from risk management to legal compliance, business alignment, and protection against evolving threats. This comprehensive approach forms a robust foundation for MHC's information security framework, supporting its smooth transition into the e-business era while safeguarding the integrity and confidentiality of its data.

6.0 MHC Security Policies Examples

Policy 1 - Acceptable Use Policy for Corporate Internet Usage

This policy defines the guidelines and expectations for the appropriate use of Internet resources; applying to all employees, contractors, consultants, temporary workers, and other affiliated personnel with Munkirk Hayern Corporation (MHC). The usage of the Internet is allowed and encouraged when it helps the company achieve MHC's business goals and objectives while ensuring a secure, effective, and respectful work environment.

Standards:

The standards outline the unacceptable behaviors of the Internet by all of MHC's affiliated personnel. The standards ensure that all personnel must comply with current legislation, appropriately use the Internet, and do not create unnecessary risks to the company. Access to the Internet using MHC-owned computers outside of MHC's network must adhere to the same policies that apply to use from within MHC's facility.

Here are some of the unacceptable uses of the Internet (not limited to):

- browsing Internet websites that have offensive, hateful, or pornographic materials
- committing any form of fraud, or software or music piracy
- sending unpleasant or disturbing content to other users via the Internet
- hacking into unauthorized websites or areas
- intentionally engaging in tasks that waste employee's time or shared resources
- bringing computer viruses or malware of any kind into the company's network
- communicate confidential or internal information via the Internet
- engaging in unapproved activities: recreational games, streaming media, personal social media, etc

Procedures:

- **Monitoring:** MHC acknowledges that Internet usage is a vital tool for their business needs. However, improper use of this resource may harm staff output and the company's reputation. Hence, MHC maintains the right to monitor all volumes of the Internet network traffic and the websites that are visited. If there is suspicion of improper use, specific contents of the transaction will be monitored.

- **Sanctions:** All suspected policy violations will be investigated by the IT department. Failure to comply with these guidelines will result in sanctions ranging from disciplinary

actions such as verbal and written warnings, or temporary suspension of IT privileges, through to termination of employment.

- **Reporting:** All personnel must promptly report suspected policy violations or harmful events performed on the Internet by sending a formally written E-mail or physical meeting with the Head of the Department/ Head of the IT Department.

- **Agreement:** All of MHC's employees, contractors, or temporary staff who have been given the right to use the company's Internet must sign a softcopy agreement and submit the signed copy to the IT Department to confirm their understanding and acceptance of this policy.

Policy 2 - Security Awareness Training Policy for All Employees

This policy aims to specify MHC's internal information security awareness and training program to inform and access all employees regarding their obligations to information security. This policy applies to all MHC's employees and all affiliated personnel who have access to MHC's systems, network, and company digital and physical information. Security awareness training is mandatory for everyone, and is especially applicable to senior-level management of MHC as they are high-value targets with access to sensitive and valuable information

Standards:

- All new MHC personnel must complete the approved security awareness training class before, or at least within 15 days of, being granted access to any of MHC's Information Resources. The training should include fundamental topics on password security, physical security, anti-phishing techniques, spear-phishing, and social engineering.
- All new MHC personnel are to undergo a 2-day engaging onboarding session to understand the company security policies, company handbook, and important agreements. They must familiarise themselves with the internal policies and governmental protocols and regulations that will impact MHC.

- Besides new MHC personnel, all existing employees regardless of position must undergo an annual security awareness program. Security awareness in the company will allow employees to understand their role within the organization and get updates on new regulations and policies, covering the latest security threats and attacks.

Procedure:

- All personnel must be provided with and acknowledge they have received and agree to adhere to MHC's Information Security Policies before they are granted access to their Information Resources.

- MHC's IT Department will send out regular Google Calendar reminders about the annual Security Awareness Training for all of MHC's personnel. Periodic reminders through Email will be provided to reinforce security awareness principles. The IT department will coordinate and conduct the current and informative security training sessions.

- There will be brief assessments following the annual training to evaluate the personnel's understanding of key security concepts. The results of the assessment will help identify areas for improvement and guide future training efforts.

- Failure to complete security awareness training may result in consequences, including additional training requirements or disciplinary actions. The IT Department will ensure all of MHC's personnel have completed their annual training.

7.0 References:

Ackerman, D. (n.d.). Windows 11 review: Microsoft's subtle changes make you ask, update or wait? CNET. https://www.cnet.com/tech/computing/microsoft-windows-11-review/

Andreja Velimirovic (2023). "Debian vs Ubuntu Server: Which Distro Should You Choose?" Retrieved from https://phoenixnap.com/blog/debian-vs-ubuntu-server

Broadberry. (n.d.). "Ubuntu Server OS." Retrieved from https://www.broadberry.co.uk/server-os/ubuntu

Chin, M. (2023, October 4). These are the macOS Sonoma features you should actually pay attention to. The Verge. https://www.theverge.com/23900372/apple-macos-14-sonoma-review-mac-imac-macbook

Common macOS Sonoma problems and how to fix them. (2023, October 4). Digital Trends. https://www.digitaltrends.com/computing/how-to-fix-common-macos-sonoma-problems/

Device encryption in Windows - Microsoft Support. (n.d.). Support.microsoft.com. https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d

EC-Council. (2020, May 28). Security Awareness Training: 6 Important Training Practices. Aware.eccouncil.org. https://aware.eccouncil.org/security-awareness-training-6-important-training-practices.html

Editor. (n.d.). macOS 14 Sonoma superguide: Everything you need to know. Macworld. https://www.macworld.com/article/1670742/macos-14-release-date-features-compatibility-beta.html

FRSecure. (2021, July 29). Acceptable Use Policy Template | FRSecure. Frsecure.com. https://frsecure.com/acceptable-use-policy-template/

Group Policy (GPO) and its Role | Kisi Access Solutions. (n.d.). Www.getkisi.com. https://www.getkisi.com/guides/group-policy

Jonson, D. (2023, December 5). Exploring the Power of Windows 11 Remote Desktop Connection. Medium. https://medium.com/@davidjonson2022/exploring-the-power-of-windows-11-remote-desktop-connection-7faf65fae1df

KOURAFALOS, O. (2021, July 13). Windows 11: The Pros and Cons Everyone Is Talking About. MUO. https://www.makeuseof.com/windows-11-pros-and-cons/

macOS Sonoma brings new capabilities for elevating productivity and creativity. (n.d.). Apple Newsroom. https://www.apple.com/newsroom/2023/06/macos-sonoma-brings-new-capabilities-for-elevating-productivity-and-creativity/

Maxis. (n.d.). Contact Us. Retrieved from https://www.maxis.com.my/en/contact-us/

Microsoft. (n.d.). Compare Windows 11 Home vs Pro Versions | Microsoft. Windows. https://www.microsoft.com/en-my/windows/compare-windows-11-home-vs-pro-versions

Nonis. (2024). What is Ubuntu? Retrieved from https://monovm.com/blog/what-is-ubuntu/#:~:text=Disadvantages%20of%20Ubuntu,-There%20is%20a&text=Ubuntu%20is%20not%20a%20good,you%20might%20get%20compatibility%20issues.

Redswitches. (2023). "Amazon Linux vs Ubuntu: Which OS Should You Choose?" Retrieved from https://www.redswitches.com/blog/amazon-linux-vs-ubuntu/

techtron_adm. (2014, August 13). Sample Internet & Email Usage Policy. TECHTRON. https://techtron.co.za/sample-internet-email-usage-policy/

TIME Internet. (n.d.). For Home. Retrieved from https://www.time.com.my/for-home/?utm_source=InvolveAsia&click_id=8066316d2c54446fb94c168e6942afdc

TrustRadius. (n.d.). "Ubuntu vs Windows Server." Retrieved from https://www.trustradius.com/compare-products/ubuntu-vs-windows-server

Ubuntu. (n.d.). "Ubuntu Desktop." Retrieved from https://ubuntu.com/desktop

What is Domain Join? An Easy Guide to Setting Up and Using it | Lenovo US. (n.d.). Www.lenovo.com. Retrieved March 6, 2024, from https://www.lenovo.com/us/en/glossary/domain-join/

Windows 11 Home vs Windows 11 Pro: here are the major differences. (2021, July 26). Xda-Developers. https://www.xda-developers.com/windows-11-home-vs-windows-11-pro/

Windows 11, W. you're considering an upgrade to, Features, I. I. H. to B. F. with the N., Productivity, B. A. to Y. in T. of, performance, Windows 11, security W. you're considering an upgrade to, Features, I. I. H. to B. F. with the N., Productivity, B. A. to Y. in T. of, performance, & security. (n.d.). Should You Upgrade to Windows 11? Intel. https://www.intel.com/content/www/us/en/tech-tips-and-tricks/should-i-upgrade-to-windows-11.html

Wong (2023). Ookla crowns TIME as Malaysia's best fibre broadband provider. Retrieved from https://www.malaymail.com/news/malaysia/2023/07/18/ookla-crowns-time-as-malaysias-best-fibre-broadband-provider/80358