ADAM GATHERER
MAGIC MEMORIES
1: SECURITY UPGRADE
JANUARY 2021 - MAY 2021

CONTENTS

1.1.1 - PROBLEM ANALYSIS

Magic Memories is a Scottish company in Central Scotland which specialises in the supply of storage devices for both local and global companies. They have replaced their previous computer network with new equipment to meet their growing requirements as the company has been doing well. Currently, they have ten employees (*fig i.*).

Managing Director	R Williamson
Sales Department	
Sales Manager	M Heron
Sales Staff	R Simpson (Glasgow) L McKechnie (Edinburgh)
Purchasing Department	
Purchasing Manager	C Palmer
Purchasing Staff	M Masters G Dott
Accounts Department	
Accounts Manager	J Ingram
Accounts Staff	G Forbes (Ledgers) J Gibson (Payroll)

fig i.

While the new network is operational the Managing Director Mr Williamson has expressed concerns about security after reading numerous reports on denial of services attacks and loss/corruption of data following security breaches. For this reason, he has hired me as an external consultant to review the security of the network and propose a set of revised security procedures to cover five areas of security. The five areas are network security, compliance and operational security, threats and vulnerabilities, application data and host security, and access control and identity management. These are explained below.

THE FIVE AREAS OF SECURITY

Network Security

Security pertaining to the technical side of computer networks. Things like network device configuration, protocols in use, commonly use network ports and wireless security come into this area.

Compliance and Operational Security

Keeping in line with the legal framework and best practice guidelines surrounding computer networks. Things like ensuring correct device configuration, compliance with the Data Protection Act, risk mitigation, incident response, security awareness training for employees etc.

Threats and Vulnerabilities

These are the various ways attackers try to damage your company and the ways in which your company could be attacked. This includes malware (worms, trojans, rootkits, viruses etc.), types of attack (spam, phishing, vishing, shoulder surfing, dumpster diving, wireless attacks, social engineering), how to detect these threats/vulnerabilities and how to mitigate them.

Application, Data and Host Security

The securing of applications, the protection of data and the hardening of hosts. Think drive encryption, anti-malware software, hardware security (cable locks for PCs, locking network cabinets), data loss prevention, group policy to prevent users accessing data they don’t need to, locking computers when stepping away from the desk.

Access Control and Identity Management

This comes down to making sure only the people you want can access sensitive data and ensuring they are who they claim to be. This is done with user accounts, passwords, two-facto authentication methods, AAA (authentication, authorisation, accounting), keeping security logs, implicitly denying access, and adding permissions as needed, password policy (complexity, length etc.).

INFORMATION GATHERED

To aid in my review of the computer network I had a question and answer session with the managing director (full transcript included in section 1.1.7), took a staff list (*fig i*), obtained company network diagrams (*fig ii*), took inventory of current equipment (*fig iii*), drew up a floorplan of the office (*fig iv*) and took note of their current addressing scheme (192.180.100.0/24, DHCP on router).

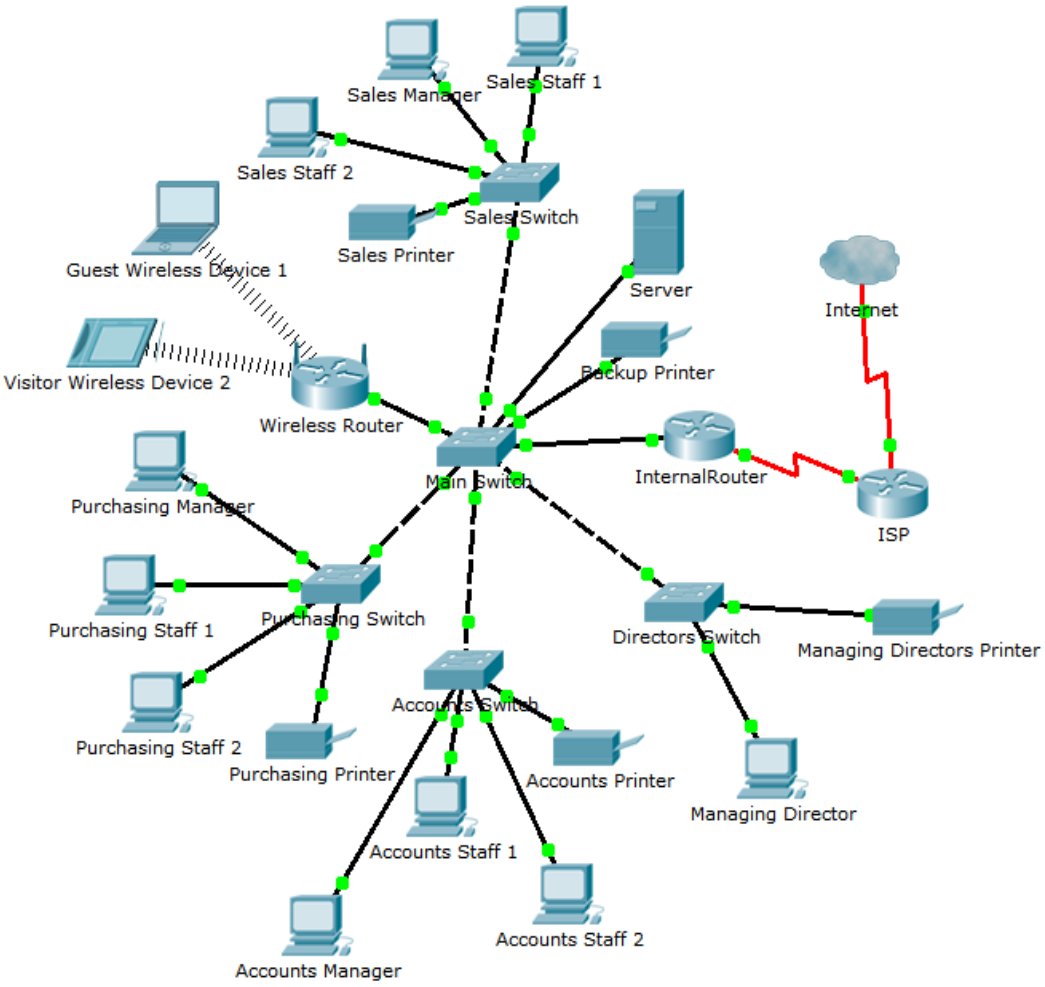

fig i - the current Magic Memories network

Item	**Name**	**Information / specification**
Routers	Internal Router	Cisco 2901 router (IOS 15.0)
	Wireless Router	Linksys WRT 1900 ACS Wi-fi Router
	ISP	Unknown (because it is not our router)
Switches	Main Switch	Cisco Catalyst 2960 24 TC-L Switch
	Sales Switch	Cisco Catalyst 2950 WS-C2950G 24 Port Switch
	Purchasing Switch	Cisco Catalyst 2950 WS-C2950G 24 Port Switch
	Accounts Switch	Cisco Catalyst 2950 C2950T-24 24 Port Switch
	Directors Switch	Cisco Catalyst 2960 24 TC-L 24 Port Switch
Server	Server	HP XW6600 E5450 3.00GHz Twin Quad Core, 16GB RAM, SATA RAID 1x 500MB HD, 2x 1TB HD
PCs	Sales Manager	Dell Optiplex 790 i5 3.1GHz, 8GB RAM, 500GB HD
	Sales Staff 1	Dell Optiplex 740 AMD Athlon 64 3800+ 2.4GHz, 4GB RAM, 160GB SATA HD
	Sales Staff 2	Dell Optiplex 740 AMD Athlon 64 3800+ 2.4GHz, 4GB RAM, 160GB SATA HD
	Purchasing Manager	Dell Optiplex 790 i5 3.1GHz, 8GB RAM, 500GB HD
	Purchasing Staff 1	Dell Optiplex 740 AMD Athlon 64 3800+ 2.4GHz, 4GB RAM, 160GB SATA HD
	Purchasing Staff 2	Dell Optiplex 740 AMD Athlon 64 3800+ 2.4GHz, 4GB RAM, 160GB SATA HD
	Accounts Manager	HP Pro 4300 i3 3.3GHz, 4GB RAM, 250GB HD
	Accounts Staff 1	HP Pro 4300 i3 3.3GHz, 4GB RAM, 250GB HD
	Accounts Staff 2	HP Pro 4300 i3 3.3GHz, 4GB RAM, 250GB HD
	Managing Director	Dell Optiplex 790 i5 3.1GHz, 16GB RAM, 500GB HD
Printers	Sales Printer	HP Colour Laserjet 555DN
	Purchasing Printer	HP Business Inkjet 2800
	Accounts Printer	HP Laserjet P4015n
	Managing Directors Printer	HP Colour Laserjet 555DN
	Backup Printer	HP Business Inkjet 1000

fig iii - list of current equipment

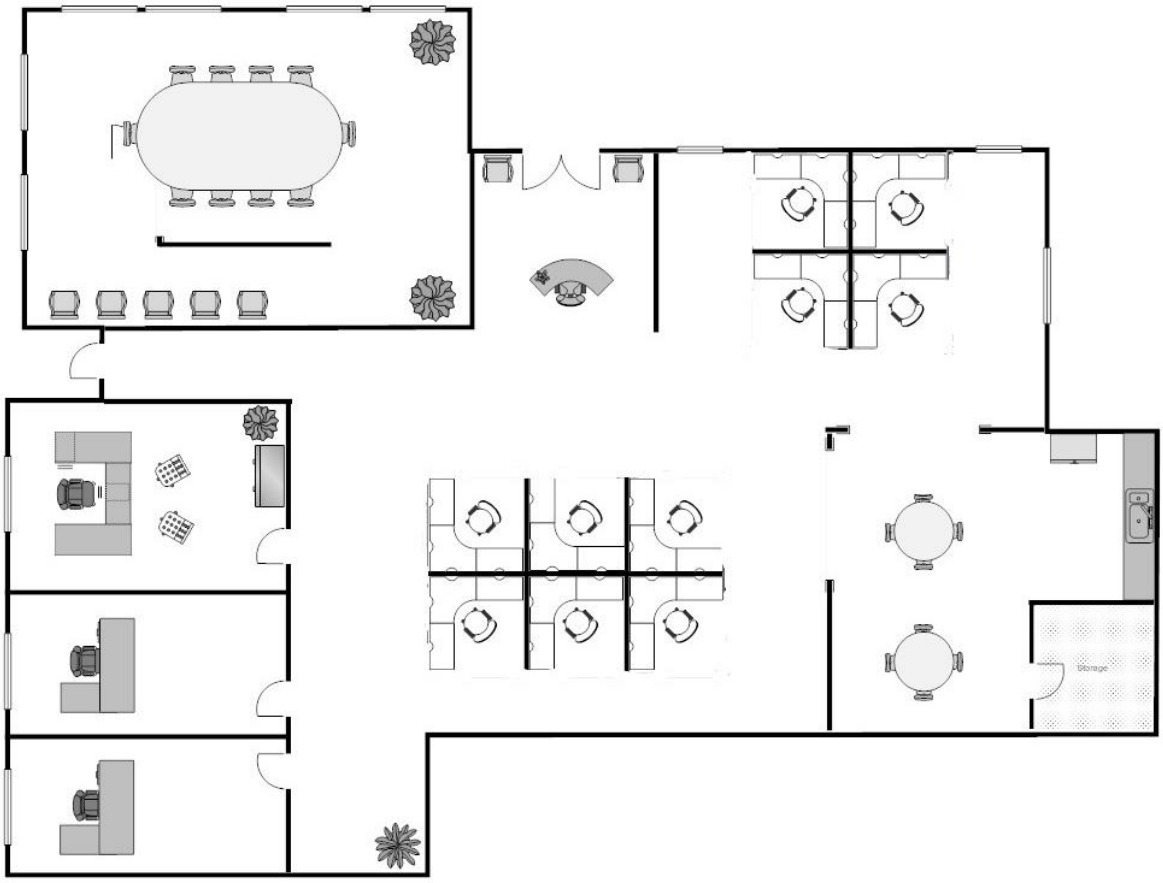

fig iv - floorplan of the Magic Memories office, details below

Work areas:
Meeting room, office entrance door / entrance area and reception desk, Sales team desks (4 desks).
Managing Directors office (lager desk), Sales manager office (smaller desk), empty office (with desk).
Purchasing and Accounts team desks (6 desks). Kitchen area, store room.
Office space: 15 metres x 20 metres (approximate).

PROBLEMS IDENTIFIED

Through my analysis of the current network and an interview with the managing director I have identified a list of security faults. I have listed the faults below and will propose fixes for them in section 1.1.7.

Network Security (NS)

1. All devices are in the same network without any subnetting.
    a. This means devices will have access to the whole subnet without any control over which devices can access which parts of the network (eg, all staff can access manager's printer). [1]
    b. The broadcast domain is the size of the entire networking, which can lead to traffic congestion, reduce efficiency [1], and leave the network vulnerable to ARP spoofing. ARP spoofing is used as an opening for denial of service attacks. [2]
2. No use of VLANs for each of the departments
    a. Causes a large broadcast domains and prevents the logical moving of computers to different departments. [3]
    b. Devices can receive broadcasts intended for other devices, vulnerable to ARP spoofing. [3]
3. No passwords set on routers/switches
    a. Unauthorised users can make changes to the devices.
4. Network traffic is unregulated
    a. A lack of a firewall or ACLs means any and all traffic is permitted to travel to any destination through any switchport on the network.
5. Network ports are left open
    a. There are 65535 ports available and each port is a way for an attacker to attempt to enter your network. Closing unused ports keeps potential threats closer to the realm of the known. Changing commonly used ports (especially SSH access) will prevent any opportunistic attacks. [4]
6. NAT is not implemented on the ISP router
    a. Internal host IP addresses can be seen by external devices. [5]
7. The wireless network has several problems
    a. WPA2 is not in use
        i. WPA is not as secure as WPA2, which uses AES encryption and longer passwords to be more secure than WPA. WPA is not ideal for enterprise bussiness use. [6]
    b. DHCP options left at default
        i. As per the interview with the Managing Director, the wireless. Traffic is approximately 20 users per day. If the lease time is not reduced this could easily exhaust the supply of IP addresses, creating an accidental DHCP starvation attack. [7]
    c. Wireless access point is on the front desk
        i. The aim is to keep as much of the wireless network within the confines of the building itself as possible. Currently, potential attackers need only be outside the bnuilding in order to attack the Wi-fi network. The router, however, has an operating range of 300ft, making finding the optimal position difficult. [8]

Compliance and Operational Security (C&OpSec)

1. No privacy policy for customer data
    a. As the website collects data on the customers for commercial use a privacy policy is required as per the Data Protection Act 1998. [9]
2. No policy on personal devices
    a. Personal devices cannot be guaranteed to be as safe as company devices, can be misplaced, and bring inconsistencies into the tools available to staff (eg, a personal laptop cannot run the accountancy software). [10]
    b. Personal data cannot be stored on personal devices, so data will have to be downloaded, uploaded and removed every time it is needed. Personal devices will also have to have information wiped from them as employees leave the company. [11]
3. No company policy on access to social media
    a. Social media distracts employees, can be used to leak confidential information (intentional or otherwise), and can expose users to risks such as viruses and phising attacks. [4]
    b. To prevent too much of a dip in morale, employees should be allowed access via their personal internet connection (eg, smartphone) on their personal time (eg, breaks).
4. Infrequent backup policy
    a. As per the interview with the managing director Magic Memories only backs up data once every three months. This is not frequent enough to mitigate a serious loss of data. Data should be backed up at *least* weekly. [5]
5. Employees have open workspaces/desks
    a. Sensitive information can wind up placed in plain sight, violating the Data Protection Act. Excessive paperwork on desks can leave visitor with bad first impressions, and increase employee stress and paper waste (ties into secure disposal of documents, see T&V 8.). [6]
6. Lack of documented fire suppresion system
    a. While not required under UK law, a Fire Risk Assessment may result in one being needed. Also vital for protecting server against fire. [7]
7. Ambiguous documentation of ethernet cables' EMI shielding
    a. Unshielded cabling suffers from cross-talk and can even have network information read by EMI detecting devices. Cross-talk and intereference also decrease network performance. [8]

Threats and Vulnerabilities

1. The previous contractor left free anti-malware
    a. With free anti-malware the protection, security features and technical support are minimal. Paid anti-malware software is more suitable for the protection of critical data. [1]
2. Public IP address exposed to DNS servers
    a. Attackers can see web server IP address.
    b. Malicious traffic can make it directly to the web server without third party intervention. [2]
    c. DDoS attacks can make it all the way to Magic Memories' internet connection without being stopped. [2]
3. Staff unaware of social attacks (spam, phishing etc.)
    a. The end users are the weakest element of a computer network if not properly trained. Almost a third of phising emails are opened and one in ten employees will click on malicious links if not trained otherwise. [3]
4. No switchport security configuration (MAC filtering, unsured switchports left enabled etc.)
    a. Limiting the MAC addresses prevets unknown devices connecting. [4]
    b. Leaving unusued ports enabled leaves devices at risk of on-site attacks. [4]
5. No ID badge policy
    a. Having staff ID badges on display at all times fosters a sense of security and makes access and tracking easier. [5]
6. Access, events and security logs are not kept
    a. Without keeping logs it is harder to detect suspicious activity. [6]
7. No privacy filters for staff computers in open area
    a. Shoulder surfing can result in attackers seeing passwords and sensitive data, endangering the private data of Magic Memories and their customers. [7]
8. Documents are not shredded before disposal
    a. This leaves the company vulnerable to dumpster diving attacks.
    b. Attackers can obtain private information for use in other attacks (social engineering, for example). [8]
    c. Enhances client trust with good security practices. [8]

Application, Data and Host Security

1. Anti-malware software is not installed on every device
    a. Malware is a serious threat to data integrity. Many types of malware can transmit private data across the internet under the guise of regular traffic. [1]
    b. Anti-malware can play a key part in preventing ransomware, keeping data safe from loss or corruption. [2]
2. Network Cabinets are left unlocked
    a. Locking cabinet netowkr cabinets provides an extra layer of security against any on-site attackers. [3]
3. Hard disks are unencrypted
    a. If any company hard drives are misplaced or stolen attackers can easily access all data if the drive is not encrypted. [4]
4. Employees do not lock computer screens when leaving their desks
    a. With staff in open areas an attacker need only walk in the front door and have access to their computers.
    b. Confidential information can be accessed and saved to removable storage. [5]
    c. Attackers can alter files or install malware directly to a user account. [5]
5. No cable locks for computers
    a. Attackers can simply walk in and remove a device.

Access Control and Identity Management

1. No use of biometric authentication
    a. Biometric measures are near impossible to replicate, cannot be stolen and are convenient for users. [1]
2. No time of day restrictions
    a. Staff below management level are only meant to have local access between 0800 and 1800, as per the interview questions with the managing director.
3. As per the interview with the managing director, there is no password policy in place
    a. Employees could be reusing using passwords for everything, meaning that if a seemingly unrelated password is obtained then their employee accounts are compromised. [2]
    b. Employees could be using insecure passwords to save on remembering something more complex. [2]

1.1.2 - PROJECT AIMS

The aim of the project is to review the current network, put forward a set of security recommendations and implement changes to harden the network.

The review will be achieved by reading the project brief and clarifying my understanding via interviews with the directing manager, consulting the current network diagrams, examining the equipment in use, and using this information to build a bigger picture of the security in place.

This model will be cross-referenced against my personal body of computer security knowledge and the information available to me through my college education and personal research. Any areas found lacking will be the output of the review and from there the implementations and recommendations can be developed. The most important changes will be implemented into a virtual recreation of the computer network to demonstrate their value, and the remainder of the changes shall be listed as recommendations.

In addition to the upgrade to the Magic Memories network I will also be developing my computer networking skills, improving my report writing, and bolstering my overall experience. My ability to write a cohesive document will benefit from this experience, as will my self-evaluation. These areas are vital for progression to university and starting my career as a network engineer.

1.1.3 - PROJECT REQUIREMENTS

Before being considered complete, the upgrade project must meet several requirements. These can be categorised as either functional or non-functional requirements.

FUNCTIONAL REQUIREMENTS

Staff departments should be divided up into separate networks via subnetting and VLANs to control inter-department access to services and resources.

All employees will have their own PCs with an office suite and should be able to use the backup printer and access their private data storage. Managers have access to all files within their departments. The directing manager should have access to all files and data.

Each department will only have access to their own printers, with the managing director having his own personal printer.

Sales staff should have sales ledger software, contact management software and sales tracking software. The sales department manager should have access to the web development software.

The purchasing department staff will have purchase ledger software and full internet access.

One member of the accounting staff will have payroll management software, another will have a standard accounting package.

The managing director and all department managers will have full internet access. Other departments (excluding purchasing) shall be restricted to email only.

All managers are permitted remote access to the network at any time and the employee in the Glasgow office should be able to access the network remotely. This will be implemented via the VPN (as per interview with managing director).

All other staff are only allowed local access between 0800 and 1800.

The network will be secured by purchasing firewall to finely tune inbound and outbound traffic, as per the interview with the managing director.

The wireless portion of the network will be set up on its own subnet and have its security hardened with WPA2 encryption. It should also be able to manage up to 20 guest users per 24 hours.

Protections should be put into place on all networking devices to mitigate network attacks, including securing switchports and implementing ACLs. Access to

networking devices such as routers and switches shall be severely limited and secured from attacks.

Anti-malware and anti-virus software will be installed onto all devices and regularly maintained and updated.

A secure password policy shall be implemented, requiring user passwords to be complex yet memorable. User accounts and passwords are to be managed and maintained on a central Windows Server, as per the interview with the managing director.

System updates and backups will be scheduled on a weekly basis as once every 3 months is far from secure.

The data storage and company information will be protected from external attacks and general data loss/corruption.

NON-FUNCTIONAL

Enhance security and network resilience with consideration to the five areas of computer security, as per the interview with the managing director.

Ensuring the network security recommendations are scalable to match company growth

Preventing data loss/corruption, either through internal or external threats. This can also be achieved through the regular backups, allowing for easier and faster recovery should anything go catastrophically wrong

Through securing the network there will be an increase in staff confidence. This can be fostered by ensuring employees are updated on the changes being made and how those changes affect their day-to-day working lives and how the changes help the company.

Security changes should be made aware to clientele as well (although in vaguer, simpler terms) to improve their confidence in Magic Memories.

By implementing the security recommendations, the company will have a faster response time, greater recovery prospects and minimal damages in the event of an attack.

Adding in redundant connections between the department switches will increase network reliability and allow for a faster, more efficient computer network, further increasing employee confidence.

CONSTRAINTS

The project will have some constraints that limit how it will progress.

- The time limit for the project (3 months) will limit how long can be spent on planning and developing the ideas used in the upgrade.

- The spending budget of £5,000 affects what can be purchased for the upgrade. The details of this are included in a table at the end of this section

- The experience of the network engineer (i.e. me) will inhibit the possible solutions. I will work to the best of my ability and believe my competence is enough to achieve the security goals.

SPENDING BUDGET				
ITEM		SOURCE	COST	TOTAL
Firewall				
	MSI B450M mATX Motherboard	Ebuyer[1]	£79.98	£79.98
	Thermaltake Level 20 VT Micro ATX Case	Ebuyer[2]	£93.99	£173.97
	Patriot Signature DDR4 16GB RAM	Ebuyer[3]	£61.62	£235.59
	2x StarTech PCIE Gigabit Ethernet NIC	Ebuyer[4]	£39.32 (£19.66 x2)	£274.91
	Thermaltake TR2 500W Power Supply	Ebuyer[5]	£32.98	£307.89
	AMD Ryzen 5 2600 AM4 CPU	Ebuyer[6]	£169.98	£476.87
	Seagate BarraCuda 1TB Desktop Hard	Ebuyer[7]	£32.99	£509.86
Category 5E UTP Network Cable 200M		TLC Direct[8]	£22.40 (£11.20 x2)	£532.26
20x RJ45 Cat 5E Plugs - 8 Way		TLC Direct[9]	£3 (£0.15 x20)	£535.26
Round Clips 3-5mm		TLC Direct[10]	£1.99	£537.25
Dell PowerEdge R340 Rack Server		EuroPC[11]	£949.99	£487.24
Cisco WS-C3560-24PS-S Switch		Best4Systems[12]	£325.00	£1812.24
Bitdefender GravityZone Business Security (3 year subscription)		Bitdefender[12]	£405.99	£2218.23
3M Gold Privacy Filter x 12		Staples [13]	£623.88 (£51.99 x 2)	£2842.11
USB Combination Lock x 12		CPC [14]	£152.16 (£12.68 x12)	£2994.27

BUDGET SOURCES

[1] https://www.ebuyer.com/911265-msi-ryzen-b450m-mortar-max-am4-matx-motherboard-b450m-mortar-max

[2] https://www.ebuyer.com/860398-thermaltake-level-20-vt-micro-atx-case-ca-1l2-00s1wn-00

[3] https://www.ebuyer.com/900773-patriot-signature-premium-ddr4-16gb-2x8gb-2666mhz-pc4-21300-udimm-kit-w-heatshield-psp416g2666kh1

[4] https://www.ebuyer.com/584553-startech-com-1-port-pcie-network-card-low-profile-gigabit-ethernet-server-st1000spex2l

[5] https://www.ebuyer.com/788081-thermaltake-tr2-s-series-500w-power-supply-80-plus-ps-trs-0500npcwuk-2

[6] https://www.ebuyer.com/830816-amd-ryzen-5-2600-am4-processor-with-wraith-stealth-cooler-yd2600bbafbox

[7] https://www.ebuyer.com/758013-seagate-barracuda-1tb-3-5-hard-drive-at-ebuyer-com-st1000dm010

[8] https://www.tlc-direct.co.uk/Products/CACAT5Eslash100.html

[9] https://www.tlc-direct.co.uk/Products/CX215R.html

[10] https://www.tlc-direct.co.uk/Products/CCRC3.html

[11] https://www.europc.co.uk/dell-poweredge-r340-rack-server-silver-intel-xeon-e-2224-16gb-ram-3x-1tb-sata-dvd-rw-dell-3-yr-wty-145405.html

[12] https://www.bitdefender.co.uk/business/smb-products/business-security.html

[13] https://www.staples.co.uk/office-supplies-and-stationery/electronics/computer-accessories-and-peripherals/computer-screen-privacy-filters/3m-black-privacy-filter-for-desktops-19in-widescreen-16-10-pf19-0w/

[14] https://cpc.farnell.com/hama/00054117/usb-notebook-combination-lock/dp/CS30860

1.1.4 - KEY FACTORS

The completion of the project is dependent upon meeting the requirements (see 1.1.3) and to do so will mean navigating the influences of the following factors.

- The equipment provided by Magic Memories (as listed in 1.1.1, *Information Gathered*) defines most of the devices used. These are the devices that make up the network and are the ones to be secured.

- The purchasing budget of £5,000 (as per the interview with the managing director) will allow for additional equipment to be purchased where necessary.

- The managing director has specifically expressed concerns over denial of service attacks and loss or corruption of data.

- As per the interview questions with the managing director, the security recommendations must be made in accordance with the five areas of computer security.

- An important factor is to keep the project within scope; while upgrading all areas of security (eg, not spending a lot of time identifying weaknesses in physical security as this is outside the scope of the project).

- Mentioned in the previous section (1.1.3) the timescale is 3 months to plan, develop, test, and evaluate the network security upgrade project.

- The client needs are detailed in the requirements section (1.1.3) of the project and outline what is to be done with the network.

- The diverse resources required to provide the upgrade (such as network simulation/emulation software, virtual machines for prototyping servers etc.) will have an impact on how the project is completed. More details on the available resources are in the next section (1.1.5).

1.1.5 - RESOURCES AND MATERIALS

The following resources will be required for the project:

- EVE-NG network emulator server to prototype the wired network (a free community version is available via eve-ng.com).

- Packet Tracer network simulation software to prototype the wireless network (downloaded via Cisco Networking Academy).

- VMWare virtualization software to host the EVE-NG server and prototype the Windows and Linux servers (VMWare Workstation license provided by Edinburgh College).

- The following operating systems: Windows Server 2019, Windows 10, Debian 10.8.0, EVE-NG, PfSense 2.5.0 (Microsoft operating system licenses provided by Edinburgh College, the rest of the software is free open-source software available for anyone to download).

- Microsoft Office Suite for word processing (Word), spread-sheets (Excel), and diagrams (Visio) (licenses provided by Edinburgh College).

For information sources outside of the project brief (listed in section 1.1.6, *Information Sources*) an internet connection and access to books on network security will be required (CompTIA Security+ guides available in digital format, obtained via Edinburgh College, and my own personal copy).

Another resource is the human effort involved, such as the interview with the managing director, the help from college lecturers and my own expertise as a network engineer.

Given the scope of the project and the timescale it is only necessary for one network engineer to work on this upgrade. This significantly lowers the cost both in terms of human resources and the resources listed in this section.

1.1.6 - INFORMATION SOURCES

GENERAL SOURCES

Diagram of current network, staff list, equipment list and office layout supplied by Magic Memories.

Cisco. 2021. What is network security - Cisco. [ONLINE] Available at: https://www.cisco.com/c/en_uk/products/security/what-is-network-security.html. [Accessed 15 February 2021].

Dulaney, E., 2008. CompTIA Security+ Deluxe Study Guide. Wiley.

Matthias Rohr: Functional vs. Non-Functional Security Requirements. 2021. Matthias Rohr: Functional vs. Non-Functional Security Requirements. [ONLINE] Available at: http://matthiasrohr.blogspot.com/2011/11/functional-vs-non-functional-security.html. [Accessed 20 February 2021].

How Often Should You Backup Your Files?. 2021. How Often Should You Backup Your Files?. [ONLINE] Available at: https://www.datarecoverylabs.com/company/resources/how-often-should-you-backup-your-files. [Accessed 01 March 2021].

phoenixNAP Blog. 2021. 7 Proven Tactics To Prevent DDoS Attacks In 2021. [ONLINE] Available at: https://phoenixnap.com/blog/prevent-ddos-attacks. [Accessed 01 March 2021].

TrustedSec. 2021. Three Most Common Physical Security Flaws (and How to Fix Them) | TrustedSec. [ONLINE] Available at: https://www.trustedsec.com/blog/three-most-common-physical-security-flaws-and-how-to-fix-them/. [Accessed 01 March 2021].

KwekuA. 2021. Password policy recommendations - Microsoft 365 admin | Microsoft Docs. [ONLINE] Available at: https://docs.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations. [Accessed 01 March 2021].

https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

Ollam, D. 2016. The Search for the Perfect Door (title in italics). Shakacon, July 13th, Honolulu

Cover image from Freepik (flaticon.com)

NETWORK SECURITY

[1] What is Subnetting, Benefits, and How does it Work?. 2021. What is Subnetting, Benefits, and How does it Work?. [ONLINE] Available at: https://www.fieldengineer.com/skills/subnetting. [Accessed 03 March 2021].

[2] library.netapp.com. 2021. No page title. [ONLINE] Available at: https://library.netapp.com/ecmdocs/ECMP1401193/html/GUID-C9DA920B-F414-4017-8DD1-D77D7FD3CC8C.html. [Accessed 03 March 2021].

[3] RoseHosting. 2021. How and Why to Change the Default SSH Port on Linux - RoseHosting. [ONLINE] Available at: https://www.rosehosting.com/blog/how-and-why-to-change-the-default-ssh-port-on-linux/. [Accessed 03 March 2021].

[4] Cisco CCNA – NAT Advantages & Disadvantages – CertificationKits.com. 2021. Cisco CCNA – NAT Advantages & Disadvantages – CertificationKits.com. [ONLINE] Available at: https://www.certificationkits.com/cisco-certification/ccna-articles/cisco-ccna-network-address-translation-nat/cisco-ccna-nat-advantages-a-disadvantages/. [Accessed 03 March 2021].

[5] Panda Security Mediacenter. 2021. WPA vs WPA2: Which WiFi Security Should You Use? - Panda Security Mediacenter. [ONLINE] Available at: https://www.pandasecurity.com/en/mediacenter/security/wpa-vs-wpa2/. [Accessed 03 March 2021].

[6]

[7] TechCrunch. 2021. This Monstrous Linksys WRT1900AC Router Is For Folks With A Real Appetite For Networking – TechCrunch. [ONLINE] Available at: https://techcrunch.com/2014/04/29/linksys-wrt1900ac-review/. [Accessed 03 March 2021].

COMPLIANCE AND OPERATIONAL SECURITY

[1] Data Protection Act 1998. 2021. Data Protection Act 1998. [ONLINE] Available at: https://www.legislation.gov.uk/ukpga/1998/29/contents/enacted. [Accessed 03 March 2021].

[2] The Alexander Group. 2021. Bring Your Own Device" (BYOD) is a Very Bad Idea - The Alexander Group. [ONLINE] Available at: https://www.thealexander-group.com/information-technology/5-reasons-bring-device-byod-bad-idea/. [Accessed 03 March 2021].

[3] Guru in a Bottle. 2021. Why BYOD in the workplace is such a bad idea. [ONLINE] Available at: https://www.guruinabottle.com/why-byod-in-the-workplace-is-such-a-bad-idea/. [Accessed 03 March 2021].

[4] HR Daily Advisor. 2021. Pros and Cons of Banning Social Media Use at Work - HR Daily Advisor. [ONLINE] Available at: https://hrdailyadvisor.blr.com/2016/05/25/pros-and-cons-of-banning-social-media-use-at-work/. [Accessed 03 March 2021].
phoenixNAP Blog. 2021. 7 Proven Tactics To Prevent DDoS Attacks In 2021. [ONLINE] Available at: https://phoenixnap.com/blog/prevent-ddos-attacks. [Accessed 01 March 2021].

[5] Dallas Texas - Total IT. 2021. How Often Should You Perform A Data Backup? - Total IT. [ONLINE] Available at: https://totalit.com/how-often-should-you-perform-a-data-backup/. [Accessed 17 March 2021].

[6] Pure Office Solutions. 2021. The Benefits of a Clean Desk Policy | Pure Office Solutions. [ONLINE] Available at: https://www.pureofficesolutions.co.uk/clean-desk-policy/. [Accessed 03 March 2021].

[7] Conditioned Environment Mechanical Services. 2021. What are the legal requirements for fire suppression systems? - Conditioned Environment. [ONLINE] Available at: https://www.conditioned-environment.co.uk/news/what-are-the-legal-requirements-for-fire-suppression-systems/. [Accessed 03 March 2021].

[8] Cables.com. 2020. Shielded vs. Unshielded Ethernet Cable. [ONLINE] Available at: https://www.cables.com/cablesblog/shielded-vs-unshielded-ethernet-cable.html. [Accessed 3 March 2021].

THREATS AND VULNERABILITIES

[1] Difference between Free and Paid Antivirus | Free Antivirus vs Paid Antivirus. 2021. Difference between Free and Paid Antivirus | Free Antivirus vs Paid Antivirus. [ONLINE] Available at: http://www.differencebetween.info/difference-between-free-and-paid-antivirus. [Accessed 19 March 2021].

[2] Cloudflare Help Center. 2021. How does Cloudflare work? – Cloudflare Help Center. [ONLINE] Available at: https://support.cloudflare.com/hc/en-us/articles/205177068-How-does-Cloudflare-work-. [Accessed 24 March 2021].

[3] Social Engineering Explained: Reduce Your Employee Cyber-Security Risk. 2021. Social Engineering Explained: Reduce Your Employee Cyber-Security Risk. [ONLINE] Available at: https://blog.usecure.io/employee-social-engineering. [Accessed 20 March 2021].

[4] What is port security and how does it work with my managed switch? | Answer | NETGEAR Support. 2021. What is port security and how does it work with my managed switch? | Answer | NETGEAR Support. [ONLINE] Available at: https://kb.netgear.com/21786/What-is-port-security-and-how-does-it-work-with-my-managed-switch. [Accessed 20 March 2021].

[5] Badges Plus. 2021. ! ID Badges | Badges Plus Ltd. [ONLINE] Available at: https://www.badgesplus.co.uk/blog/article/why-you-should-wear-id-badges-in-the-workplace_35. [Accessed 20 March 2021].

[6] SecurityMetrics. 2021. The Importance of Log Management. [ONLINE] Available at: https://www.securitymetrics.com/blog/importance-log-management. [Accessed 20 March 2021].

[7] IONOS Digitalguide. 2021. Shoulder surfing: explanation and countermeasures - IONOS. [ONLINE] Available at: https://www.ionos.co.uk/digitalguide/server/security/shoulder-surfing/. [Accessed 20 March 2021].

[8] Signal Financial Federal Credit Union. 2021. Ten Reasons Shredding is Important | Signal Financial Federal Credit Union. [ONLINE] Available at: https://www.signalfinancialfcu.org/blog/ten-reasons-shredding-important/. [Accessed 20 March 2021].

APPLICATION, DATA AND HOST SECURITY

[1] Antivirus Insider. 2021. Benefits of Antivirus Programs - Antivirus Insider. [ONLINE] Available at: https://antivirusinsider.com/benefits-of-antivirus-programs/. [Accessed 22 March 2021].

[2] SafetyDetectives. 2021. Can Antivirus Prevent Ransomware?. [ONLINE] Available at: https://www.safetydetectives.com/blog/can-antivirus-prevent-ransomware/. [Accessed 22 March 2021].

[3] TechRepublic. 2021. Lock IT Down: Don't overlook physical security on your network - TechRepublic. [ONLINE] Available at: https://www.techrepublic.com/article/lock-it-down-dont-overlook-physical-security-on-your-network/. [Accessed 22 March 2021].

[4] TechRepublic. 2021. Lock IT Down: Don't overlook physical security on your network - TechRepublic. [ONLINE] Available at: https://www.techrepublic.com/article/lock-it-down-dont-overlook-physical-security-on-your-network/. [Accessed 22 March 2021].

[5] Weill Cornell Medicine. 2021. Lock Your Desktop When You're Away | Information Technologies & Services. [ONLINE] Available at: https://its.weill.cornell.edu/node/1596. [Accessed 22 March 2021].

ACCESS CONTROL AND IDENTITY MANAGEMENT

[1] Advantages and disadvantages of biometrics | Mitek. 2021. Advantages and disadvantages of biometrics | Mitek. [ONLINE] Available at: https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics. [Accessed 23 March 2021].

[2] lp-cdn.lastpass.com. 2021. No page title. [ONLINE] Available at: https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/logmein-lastpass-survey-ebook-v8.pdf. [Accessed 24 March 2021].

[3] Use a Passphrase. 2021. Use a Passphrase. [ONLINE] Available at: https://www.useapassphrase.com/. [Accessed 24 March 2021].

[4] Zhang, Y., Monrose, F. and Reiter, M., 2010. The security of modern password expiration: an algorithmic framework and empirical analysis. CCS '10: Proceedings of the 17th ACM conference on Computer and communications security, [Online]. Available at: https://dl.acm.org/doi/10.1145/1866307.1866328 [Accessed 24 March 2021].

[5] Scarfone, K. and Souppaya, M., 2009. Guide to Enterprise Password Management (Draft). Recommendations of the National Institute of Standards and Technology, [Online]. Available at: https://csrc.nist.gov/csrc/media/publications/sp/800-118/archive/2009-04-21/documents/draft-sp800-118.pdf [Accessed 25 March 2021].

1.1.7 - ANALYSIS

PROJECT SPECIFICATION DISCUSSION WITH MANAGING DIRECTOR

To aid in my understanding of the project requirements I took the opportunity to ask the Managing Director some questions about the upgrade. Below is a trasncript of this conversation. The questions are numbered with the Managing Director's responses indented and in a lighter font colour for clarification. Follow up questions and responses are included in the indentation in the appropriate font colours.

1 - Does this project have a budget and can we buy additional equipment?

I have £5,000 to spend on security. As I am contracting you to do the work, you can buy any additional equipment or software you think I might need to secure the current NEW network.

This is good, we will be looking to buy some more network cabling, a firewall and a small secondary server.

2 - What operating systems do you run/want to run?

We have Windows on out PCs and servers. I don't think I need to change that unless you can advise me otherwise?

We will stick with Windows for the PCs and for the main server. The server we are adding will run Linux and be used for the VPN and web hosting.

3 - Which ports are currently in use on your network?

I'm sorry, as the manager I am not an IT expert and I don't understand your question so I can't help you with that.

To clarify; what software is most commonly used? Things such as Micrsoft Outlook, accountancy software, web browsers, any specialist software that connects to the network or internet would be useful to know so we can research the ports for you. This helps with security by only permitting those programs access to specific parts of the network.

We use MSOOFFICE/OUTLOOK/SAGE.

4. - What are your static/DHCP requirements?

I'm sorry, as the manager I am not an IT expert and I don't understand your question fully. I do know however that we use the Ip address 192.168.33.0/24...does that help?

Do your employees move their computers around and about or are they plugged into the same desk? We would like to change your IP addressing to run on 10.0.0.0/24. This will not change anything for you but will make it easier for employees who deal with that sort of thing. It's a nicer number to remember than 192.something.whatever.cantmind!

5 - What security measures are currently in place and what security measures do you need implemented (other than DDoS protection)?

I would like you to consider all areas of security because the last contractor who put the network in place didn't put any security in place other than free anti-virus software which I am not happy about.

5.1 - If this is not known, can we set up security on your behalf?

Yes, I have read that there are 5 areas in security to consider so I hope you can address all of them.

This is good, we will focus on all security measures. We'll even supply physical security recommendations for free!

6 - Can we double up connections between main switch and router/server?

I'm sorry some questions you are asking are very technical. I have no idea and I hope you can design the security to the highest level possible for me please.

This just means that we will use two cables to connect the switch to the router. This makes the communication up to twice as fast and twice as reliable. If one cable fails, there's still a connection. Think of it as security against failure.

7 - What is your current password/username policy?

We don't have one.

This will be put in place. We will recreate all user accounts and enforce a modern, secure password policy. Lots of letters, numbers and symbols, set to expire every month. No doubt some employees will grumble at first, but it is better to be annoyed once a month than to have your data compromised.

8 - Do they want some sort of WAP alongside the wired setup?

We need wireless for visitors, so yes.

We will configure this for you. How many visitors do you expect on a daily basis? More than 10? 100?

We have approximately less than 20 visitors per day on Wi-Fi.

9 - How is your employee in Glasgow to connect to your network? Via a VPN or remote login?

The connection is dial up. I have heard that a VPN is the way to go? I will leave that to you, the security expert.

We will set you up with a VPN for your employee using software called OpenVPN. This will run on the Linux server and will allow pre-approved employees to connect from remote locations. It is free but regularly updated and secure.

10 - Will you need us to implement backups/redundancy?

Well as we only backup once every 3 months I think you need to change this. I don't think we need a second server for redundancy do you? Please advise me.

More regular backups will be configured for you. As for a second server this seems a bit much. With the security measures being put in place it is very unlikely that it will be taken down. Updates and backups will be configured for the middle of the night, where downtime won't affect your business.

PROPOSED SOLUTIONS

After analysis of the problems listed in section 1.1.1, I have a developed a list of security recommendations. They are listed below; with the changes I will implement listed in green and recommendations to consider listed in blue.

Network Security (NS)

1. Subnet the network by departments
    a. By subnetting the network by department no one device will have access to the whole network. [1]
    b. This also reduces the size of the broadcast domain, improving network efficiency and providing protection against ARP spoofing. [2]
2. Use VLANs for each of the department
    a. Using VLANs reduces broadcast domain size and allows computers to be moved logically from department to department. [3]
    b. Prevents devices receiving broadcasts intended for other devices, hardening against ARP spoofing. [3]
3. Configure passwords on routers/switches
    a. Prevents unauthorised users making changes to the devices.
4. Regulate network traffic
    a. Implementing a firewall and ACLs allows control over network traffic.
5. Close unused network ports and change default ports
    a. Changing the default ports for services such as SSH prevents opportunistic attacks. [4]
6. Implement NAT on the ISP router
    a. Internal host IP addresses are hidden from external devices, obscuring the network structure. [5]
7. Fix issues with the wireless network
    a. Use WPA2 encryptionon. [6]
    b. Decrase DHCP lease time to to prevent accidental DHCP starvaion. [7]
    c. Move the wireless access point to the middle of the office.

Compliance and Operational Security (C&OpSec)

1. Create a privacy policy for customer data
    a. Required as per the Data Protection Act 1998. [9]
2. Forbid use of personal devices on company network
    a. Personal devices cannot be guaranteed to be as safe and cannot hold personal data. [10] [11]
3. Forbid access to social media
    a. Social media distracts employees and poses a threat to company data. [4]
4. Configure weekly backups
    a. Weekly backups prevent loosing more than a few days worth of data in the case of a disaster. [5]

5. Implement a clear desk policy
    a. Prevents sensitive information from being spied in shoulder surfing attacks. [6]
6. Ensure fire suppresion system in place if needed
    a. Protects servers against fire and may be required as per a Fire Risk Assessment. [7]
7. Only use cables with EMI shielding
    a. Prevents cross-talk and network information being read by EMI detecting devices. [8]
8. Implement a disaster plan
    a. Weekly local backups
    b. Configure a RAID for important data storage
    c. Monthly off-site backup for recovery
        i. Useful in case of “Act of God” tier disasters.

Threats and Vulnerabilities

1. Purchase anti-malware software and implement on all devices
    a. Paid software has better support and is more suitable for the protection of critical data. [1]
2. Use a service such as Cloudflare to anonymise IP addresses
    a. Hides the public IP address of the web server and prevents traffic identified by the service as malicious from reaching the network.[2]
    b. In the event of an attempted DDoS attack, the attacker’s traffic will be directed at Cloudflare instead of Magic Memories. Cloudflare are better prepared to deal with a DDoS attack. [2]
3. Develop DDoS Response Plan
    a. List of assets to implement (threat identification software/hardware, preventions software/hardware)
    b. Response team (define who is responsible for what action)
    c. Notification procedures (who to contact in case of attack)
    d. List of on-site and off-site contacts (who to tell about the attack, such as customers, partners etc.)
4. Train staff on social attacks
    a. This protects the end user from spam, phishing etc. [3]
5. Configure switchport security on devices (MAC filtering, disable unused switchport)
    a. Mac address limiting prevets unknown devices connecting. [4]
    b. Disabling unusued ports prevents on-site attackers connecting to devices. [4]
6. Implement a policy of ID badges being visible at all times
    a. Having staff ID badges on display at all times fosters a sense of security and makes access and tracking easier. [5]
    b. Requiring guests to display ID badges makes on-site attacks harder. [5]
7. Ensure access, events and security logs are kept
    a. Keeping logs makes it easier to detect suspicious activity. [6]
8. Purchase and install privacy filters for staff computers in open area

    a. This prevents shoulder surfing and protects the private data of Magic Memories and their customers. [7]
9. Purchase a shredder for disposal of documents
    a. Prevents dumpster diving attacks from being successful. [8]
10. Physical security recommendations
    a. Harden doors
        i. Install locking pins into hinges
            1. It takes minutes to remove pins from exposed door hinges. Locking pins prevent unhinged doors from being removed.
        ii. Ensure main double door is mounted properly
            1. Entry tools are extremely thin and will fit through any gaps intruders can find.
        iii. Rotate handles 90°
            1. Prevents entry tools from pulling handles down
    b. Install window restrictors
    c. Install smart card entry system
        i. Easily monitor access

Application, Data and Host Security

1. Install anti-malware software on every device
    a. Anti-malware will protect against various malware types, including trojans, worms, viruses and ransomware. [1] [2]
2. Lock network cabinets
    a. Provides extra security against on-site attacks. [3]
3. Encrypt hard disks
    a. Protects company data in the event of hard drives being misplaced or stolen. [4]
4. Implement screen lock policy
    a. Staff in open areas no longer vulnerable to opportunistic on-site attacks. [5]
5. Install cable locks for computers
    a. Provides extra security against on-site attacks.

Access Control and Identity Management

1. Implement use of biometric authentication
    a. Biometric measures are near impossible to replicate, cannot be stolen and are convenient for users. [1]
2. Implement time of day restrictions for employees
    a. As per questions with the managing director, staff lower than managers will only be restricted to local access between 0800 and 1800.
3. Introduce a new password policy
    a. Passphrases should be used as they are more memorable while also being complex. [3]

b. Whilst mandatory password changes seem like a good idea, staff want a memorable password so for each change they are highly likely to re-use guessable elements from previous passwords. [4]
c. Mandatory password changes have been shown to be effective against only a minority of password compromises, frustrating to users and ineffective against preventing compromised passwords being used, as the attackers almost always use passwords the day they are cracked.[5]
d. Passwords should only be changed when users feel they are compromised.
e. Lockout after three incorrecct attempts

1.1.8 - PROJECT PLAN

To ensure I am on track with the upgrade I have set out a plan below. This consists of a schedule (*fig i*) with parts of the report along with a due date (in bold below) and the sub-sections of the stages with due dates of my own choosing. The major milestones in the project are also included (*fig ii*).

ITEM	DUE DATE
1 - Planning Section	**26/03/2021**
Complete sections 1.1.1 - 1.1.4	14/03/2021
1.1.5 - 1.1.9	21/03/2021
1.2	26/03/2021
2 - Development Section	**14/05/2021**
2.1 - Implement planned solution	12/04/2021
2.2 - Testing the implemented solution	19/04/2021
2.3 - Managing the project	26/05/2021
3 - Evaluation	**28/05/2021**
3.1 - Outline of the assignment	01/05/2021
3.2 - Strengths and weaknesses	08/05/2021
3.3 - Recommendations	15/05/2021
3.4 - Modifications	22/05/2021
3.5 - Knowledge and skills	28/05/2021

fig i

MILESTONE	COMPLETE
1.1.1 - All problems identified	X
Planning stage complete	X
2.1 - Network virtualised	
2.1 - Switches configured	
2.1 - Routers configured	
2.1 - Firewall configured	
2.2 Complete	
Development stage complete	
3.1 - Outline the assignment	
3.2 - 3.3	
3.4 - 3.5	
Devaluation stage complete	
Project complete	

1.1.9 - SUMMARY TABLE

NETWORK SECURITY	RECOMMENDED	IMPLEMENTED
Subnet the network		X
Implement VLANs per department		X
Set management passwords on the routers/switches		X
Purchase a hardware firewall		X
Implement ACLs		X
Restrict open ports		X
Implement NAT on the ISP router		X
Harden wireless network		X
Use WPA2-AES		X
Limit DHCP lease time		X
Move antennae	X	
COMPLIANCE AND OPERATIONAL SECURITY	**RECOMMENDED**	**IMPLEMENTED**
Create a privacy policy	X	
Forbid use of personal devices	X	
Forbid use of social media on company network	X	
Implement a disaster plan	X	
Weekly local backups		X
Configure RAID for important data storage	X	
Monthly off-site backup for recovery	X	
Implement a clear desk policy	X	
Ensure Fire suppression system is in place if needed	X	
Install security cameras in server room & entryway	X	
Use cables with EMI shielding		X
THREATS AND VULNERABILITIES	**RECOMMENDED**	**IMPLEMENTED**
Purchase anti-malware software		X
Develop DDoS response plan	X	
List of assets to implement	X	
Response team	X	
Notification procedures	X	
List of on-site and off-site contacts	X	
Foster staff awareness of social attacks	X	
Configure switchport security		X
MAC filtering		X
Disable unused switchports		X
Implement policy of staff having ID badges visible at all times	X	
Require off-site visitors to display ID badges	X	
Keep access, events, and security logs		X
Purchase privacy filters for staff in open areas		X
Purchase shredder for secure disposal of documents	X	
Only permit use of company wireless network when on-site	X	
Implement physical security changes	X	
Harden doors (locking hinges, rotate handles)	X	
Install window restrictors	X	
Install smart card entry system	X	
APPLICATION, DATA AND HOST SECURITY	**RECOMMENDED**	**IMPLEMENTED**
Purchase and install anti-malware software		X
Lock network cabinets	X	
Encrypt hard disks		X
Implement screen locking policy when employees away from		X

desk		
Purchase and install cable locks for computers	X	
ACCESS CONTROL AND IDENTITY MANAGEMENT		
Harden authentication means for sensitive areas		
Biometric authentication for server room	X	
Implement password policy changes		X
Lockout after incorrect guesses		X
Passphrases rather than passwords		X
Remove mandatory password changes	X	