By William Adoukonou

Unit 7 It system security and encryption assignment 2

Contents

[Part 1 1](#_Toc105682440)

[Part 2 7](#_Toc105682441)

[Part 3 10](#_Toc105682442)

[Test Number 1 10](#_Toc105682443)

[Test Number 2 11](#_Toc105682444)

[Test Number 3 11](#_Toc105682445)

[Test Number 4 12](#_Toc105682446)

[Test Number 5 13](#_Toc105682447)

[Test Number 6 13](#_Toc105682448)

[Test Number 7 14](#_Toc105682449)

[Test Number 8 14](#_Toc105682450)

[Test Number 9 15](#_Toc105682451)

[Test Number 10 15](#_Toc105682452)

[Test Number 11 16](#_Toc105682453)

[Test Number 12 16](#_Toc105682454)

[Test Number 13 16](#_Toc105682455)

[Test Number 14 16](#_Toc105682456)

[Test Number 15 17](#_Toc105682457)

[Feedback from Member 1 18](#_Toc105682458)

[Feedback from Member 2 18](#_Toc105682459)

[Changes Based on Client Feedback 19](#_Toc105682460)

[Updated Test Number 9 19](#_Toc105682461)

[Updated Test Number 10 19](#_Toc105682462)

[Updated Test Number 11 20](#_Toc105682463)

[Part 4 21](#_Toc105682464)

[D2 Overall Effectiveness of the Plan 21](#_Toc105682465)

[How Anti-Virus software impacted the systems security 21](#_Toc105682466)

[How WPA2 impacted the systems security 22](#_Toc105682467)

[How Software Firewalls impacted the systems security 22](#_Toc105682468)

[D3 Evidence of Individual Responsibility 23](#_Toc105682469)

# Part 1

|  |  |  |
| --- | --- | --- |
| Method | Explanation | Justification |
| Physical security | | |
| Computer/network room security | having specific security measures inside the area where secure data is held. Some examples include CCTV, Key cards and Padlocks. | This increases the security because it limits the amount of people who have access to the data. They also have 24/7 footage in case of data theft.  This can become an issue in emergency situations where the keyholder or CCTV footage can’t be accessed. This also means that the whole data relies on the holder of the key/lock. |
| Backing up data | Having multiple copies of high-risk data internally and externally. | This helps to stop the loss of data whenever is stolen or when a hardware issue occurs as there’s multiple copies saved in different places.  Having many data backups can become expensive and take up a lot of extra storage if the file size is big |
| Disaster recovery plans | Having a set out plan that is followed whenever there is a disaster e.g. earthquake, storm | This helps prevent the issue of losing data in the 1st place when combined with an external backup. If there was a storm where the main office is located and all of the hardware was destroyed, the company would be able to retrieve a copy from another location.  Again, having the resources to properly set out a good recovery plan isn’t affordable for every company. |
| Policies and procedures | | |
| Organisational policies and their application | Helps specific companies set certain rules to protect data that only applies to that industry. | It helps every company protect their data regardless of what type of data it is. For example, a bank might not employees in their vaults where large amounts of money can be stored.  This means the company to put their trust in the people who have higher access to the security data as they have the option to cause a lot of harm to it. |
| Security audits | This is When a company wants to do a system inspection to make sure all security measures are in place | Security audits from the company themselves or third parties helps the company set out a plan of what areas they need to improve on.  The issue with audits is the face that they need to be conducted by an expert who knows where there could be security vulnerabilities. |
| Default ‘factory settings’ and ‘reset’ options and backdoors | Lets the user wipe the device to the original settings so every piece of data is removed from the drive | Good as final resort option for companies that are having issues with systems such as virus attacks reverts all unfixable system changes.  This becomes a problem when the user doesn’t back up the valuable data before they restore all the data gets wiped from that specific drive. |
| Installation of software  updates, and hardware  patches and security updates | Downloading a newer version of the operating system that has fixes for security bugs there may have been | Regular software updates for your system are very beneficial as they make sure the system is always on the latest, most secure version of the OS so they aren’t exposed to any vulnerabilities.  The issue with these updates is the end goal. Every software company releases a major software update that no longer works on their older hardware. This means companies have to spend more money upgrading their system or stay on the older, less secure OS. |
| Any rules created do not impede normal business operation for an individual and the  organisation | Having certain rules in place that can jeopardise the normal business flow | Not having rules that affect business operations has a positive impact because then the business doesn’t have to slow down if any security issues meaning customers won’t be affected.  The downside to this is companies can be scared to implement these measures and then can have more security vulnerabilities in exchange for minor business operation issues. |
| Software based protection | | |
| Anti-virus software | This is specific software downloaded by the user to find and remove malicious software on a user’s computer. It also runs in the background and prevents the user from downloading suspicious files and programs | Anti-virus software acts as a user’s 2nd pair of eyes and is always scanning the system in case the user makes a mistake and downloads a file that might harm their system.  The thing with anti-virus is it usually comes as a standard version but also has better features which are locked behind a paywall. |
| Software and hardware  Firewalls | Firewalls are a form of defence for the computer system. They limit incoming and outgoing traffic on the computer to make sure no malicious code can get onto your system. | Having physical/software firewalls monitors network traffic. Since the user doesn’t have time to monitor the computer all day, the firewall does this job and prevents any virus attacks.  Although they seem very useful. Once again, cost is an issue. Firewalls that are physical or software based usually aren’t free and when they are, they might not be as thorough and advanced as paid options. |
| Intrusion detection systems (IDSs) | This is like physical alarm for threats on your computer. It uncovers the threats and alerts the user while the firewall monitors in the background. | IDSs can give you more detail about the incoming attacks whereas firewalls will just tell you the IP and ports that they are coming from. The user can then use this data to better the security of their system.  The issue is that they require someone to monitor. In order for someone to see the alert created by the IDS, a qualified technician would need to be on standby which is not always possible. |
| Domain management | Domain Management is when a person or company sets up their own domain name to register with their business and managing things such as its renewal date. | Registering domains for cases such as business purposes helps tie the specific address to your brand and makes it look more authentic.  Like IDS, they need to be monitored often. If the renewal date for your domain expires, then that specific address wont be linked to your site and people wont be able to access your webpage. |
| User authentication and  log‐on procedures | This is a websites way of proving you are the user who is requesting to log in. when you enter your details into a log in page. The server needs to know it's actually you and that you haven’t been hacked. This is where measures such as email/text 2fa come in. | User Authentication can help people in desperate situations where both the email and password has been compromised. If the login has occurred on a different machine or location, it will trigger an authentication check.  Methods such as 2fa are known to spot false positives which can lead to the user being locked out of their account when in fact, it is them trying to access the account. This can happen when a 2fa text is sent to a number that the user cannot access. |
| Access controls | Access controls are the methods that a system can use to make sure only certain people can access certain things. They come in both physical (keys, id scanners) and logical forms (group policies). | Having certain access controls in place can greatly minimize the risk of a security threat in a system. This is because people can’t access certain areas in the 1st place.  Some forms of access controls (most physical options) mean that the person has to carry their extra form of identification. This is an issue because they can be broken, lost, or even stolen. |

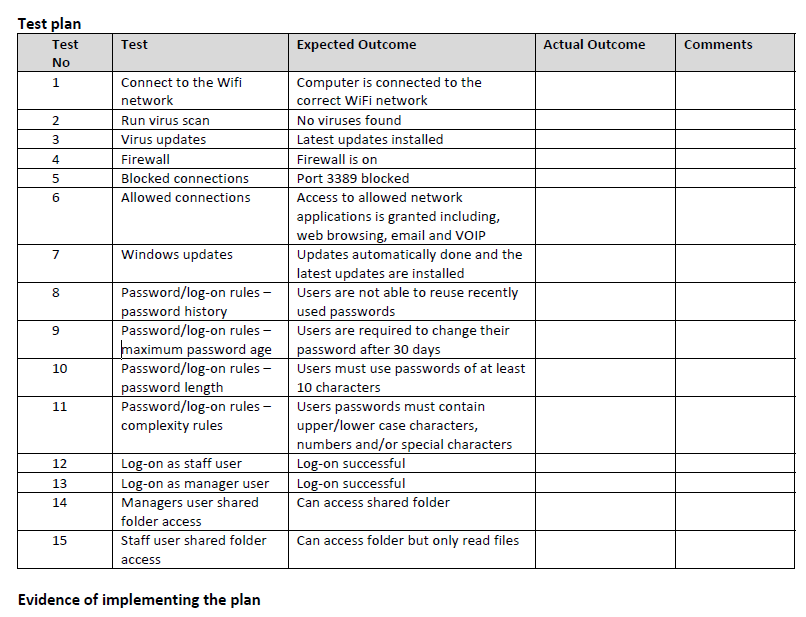
# Part 2

|  |  |
| --- | --- |
| **Task** | **Justification** |
| 1) Connect the system to the WiFi network using the correct WPA2 password and set the network profile as public | I need to be connected to the internet to download software and updates, the WiFi network sends encrypted data using the WPA2 system to prevent anyone eavesdropping on the data sent. Setting the network profile as public will help protect the system, for example this profile turns off network discovery so other computers on the network won’t see this computer. |
| 2) Install Anti‐virus software and run a system scan, check it has the latest updates | This is the most essential thing to add into the plan. Installing an antivirus software is important because it prevents malicious attacks from being carried out on the computer system. Running a system scan is also useful to do often as it checks all the files on the computer to make sure the virus hasn’t hidden itself inside a folder. |
| 3) Configure firewall | Configuring a firewall has been added to the list as it improves the network security. A firewall will actively monitor the network traffic on a network. It will also alert the user if it finds any suspicious activity. This is useful for companies with less staff as they don’t have enough people to monitor the network for long periods of time which the firewall would take care of. |

|  |  |
| --- | --- |
| 4) Check windows updates | This is the easiest thing to add to a protection plan. Checking windows updates on a computer system can greatly improve system security as it is better to be on the latest software version. Being on older software versions can put your PC at risk. This is because they are more likely to be affected by security vulnerabilities since they wont include the latest security features. |
| 5) Configure log‐on rules | Configuring log on rules should always be done when looking to improve the security of companies with multiple people. Having all your staff log in with username and passwords helps to greatly lower the risk of outside threats. All of the sensitive data would be locked away by the log in credentials so nobody could just access the computer and gain the data without hacking into the system. |
| 6) Set up user accounts and groups | This is useful for similar reasons as log on rules. Having user accounts and groups also helps separate each users’ files from each other. This will lower the chance of users losing and accidently deleting files. |
| 7) Set up a shared folder | Having a shared folder can be beneficial for companies to also keep files organised and safe. If a user wanted to set up a place to keep all important files , they could create a shared folder that way there wouldn’t be any confusion on where the specific folders would be. |
| 8) Set up file permissions | File permissions should be added the plan to help restrict access within the company. File permissions would only allow certain users to access certain files based on how sensitive the data inside is. If an employee lower down in the business needed to use a computer, they wouldn’t need permissions to access all the files on it. |
| **Things NOT included in my plan (Below are examples only, please add your own points)** | |
| Hardware firewall | Hardware firewalls have not been added to the plan because they aren’t necessary for all businesses. With software firewalls in the plan, the physical versions are just an additional cost which not all companies can afford. They also work the same way, so they aren’t that different. |
| Network/server room security | Network/server room security also hasn’t been added to the plan since they too, add an additional cost which can be expensive. If this was added, every employee who needed access to the files would need some sort of key which is not only costly, is also hard to manage with issues such as theft of the keys. |
| Domain Management | The reason why this wasn’t added was because it isn’t practical for smaller businesses. Domain management can be very useful for a businesses’ presence online however it requires a lot of monitoring. Most companies won’t have the time or people to hire to constantly manage a domain. |
| Security Audits | Even though security audits can be useful for checking the system security of your company, they haven’t been added to this plan. This is because they need to be conducted by an external expert to avoid any biases and make sure the audit is done fairly. This would also be expensive to do. |
| Default ‘factory settings’ and ‘reset’ options and backdoors | Having one of these options seems like a good last resort tool to be able to use however it can also have some negative impacts. This hasn’t been added to the plan because it could lead to an accidental data wipe. An inexperienced user who may think they need to reset the computer might accidently do it and wipe out lots of sensitive data which might not be able to be recovered. |

# Part 3

Do some research on the task and we need to provide some screenshots of doing these tasks.



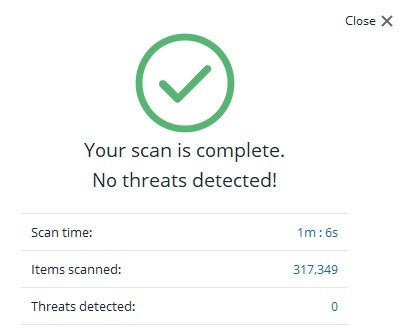
## Test Number 1

Graphical user interface, application, Teams

Description automatically generated

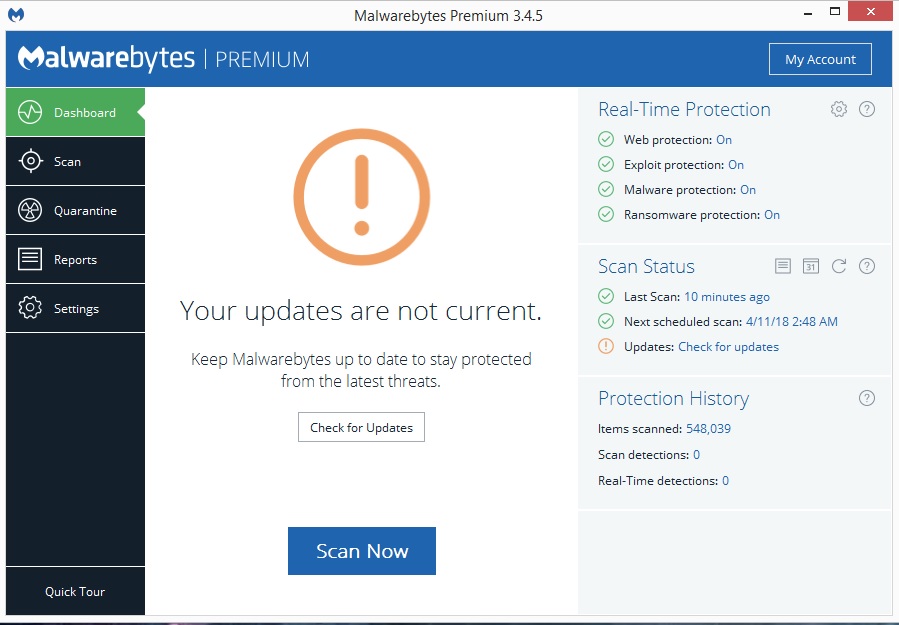
As you can see, my computer is connected to a private internet connection via Ethernet. It is important to set up an internet connection correctly as you can leave your access point vulnerable to hackers who can steal data from your computers by cracking the passcode.

## Test Number 2



After a quick scan, the computer was completely clean of threats. Its important to do these regularly so you can always be sure your computer hasn’t been compromised. Newer attacks are harder to find on your computer system alone.

## Test Number 3



A quick check of the antivirus shows that I haven’t checked for updates to the software. This is an important thing to do because these updates usually include newer methods of searching for more advanced attacks.

## Test Number 4

Graphical user interface, application

Description automatically generated

The firewall for this system is enabled for public networks and even the private network it is currently connected to. This means it will actively monitor what connections come through and block any that aren’t on the whitelist of authorised connections.

## Test Number 5

Graphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Having Port 3389 open can be dangerous to your system. It’s the port hackers can use to communicate to your system and with this, find vulnerabilities in your system that they can exploit and gain unwanted access.

## Test Number 6

Graphical user interface, text, application, email

Description automatically generated

It’s always good to keep an eye on what apps are allowed to communicate through the firewall. This is because any malicious app can easily sneak onto the whitelist which can give it the permissions to cause further damage.

## Test Number 7

Graphical user interface, text, application, email, Teams

Description automatically generated

This PC is updated and was checked recently. This is very important because these updates include security improvements so by not updating, you’re leaving yourself more vulnerable to attacks.

## Test Number 8

Graphical user interface, application, Teams

Description automatically generated

Making sure your computer system is password protected is very basic but crucial for security. Anyone can access all of your files whenever you aren’t there. They can also install spyware to run in the background and remotely steal data. A small business with a lot of crucial client data wouldn’t be able to recover from this swiftly.

## Test Number 9

Graphical user interface, text, application, email

Description automatically generated

As you can see, this computer system has the password set to never expire. For a computer that’s owned by a company that holds sensitive data, it’s really important to turn this on. If someone managed to gain access to an employee’s password. They couldn’t wait and try to log in at a later time since the password would’ve expired.

## Test Number 10

Table

Description automatically generated

The minimum password length isn’t set up. Again, for a computer that’s owned by a company that holds sensitive data, it’s really important to turn this on since a short password can be cracked a lot easier.

## Test Number 11

Table

Description automatically generated

The complexity requirements are also disabled on this machine. They should be enabled for account logins because they also make it harder to crack passwords. If the password includes a mix of capital letters, numbers, and

symbols it becomes almost impossible to guess.

## Test Number 12

Chart

Description automatically generated with low confidence

After setting up a local account for a staff user I managed to sign in. its good to set up accounts for each employee because it’s easier to manage their permissions so they can’t access information if they don’t need it.

## Test Number 13

Chart

Description automatically generated with low confidence

Now the system has been logged on with a manager account. The manager account has administrator privileges which are higher up than local accounts. This means they can access more private data which may be required for their work.

## Test Number 14

A picture containing table

Description automatically generated

The shared folder has been created and the staff user has only been given read permissions only. This means that they can’t edit any of the files or add any to the folder. This is important because the files might contain sensitive info which a regular employee could compromise it.

## Test Number 15

A picture containing table

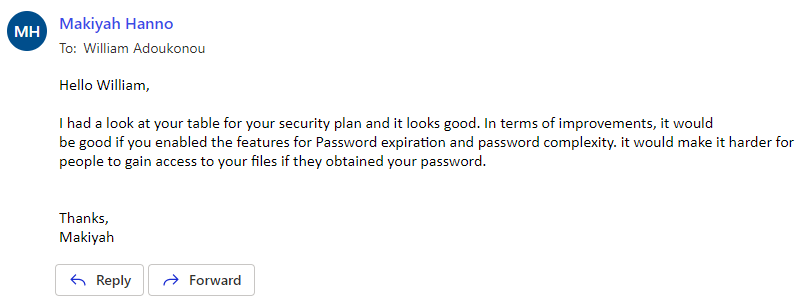
Description automatically generated

Additionally, the Manager has been added to the shared folder, but they have read and write permissions. This means that they can read the files and edit them. They can also create their own as well. Since the manager is at the top of the company, they would need access to the private files as they can be trusted.

|  |  |
| --- | --- |
| **7/D.P8** | **Review the extent to which the organisation’s IT system has been ‘protected’.** |

Take feedback from your team members (2 reviews) and show the evidence of the feedbacks (it can be email exchanges or written paragraph)

## Feedback from Member 1



## Feedback from Member 2

Text

Description automatically generated

|  |  |
| --- | --- |
| **7/D.M4** | **Enhance the protection of the IT system which to meet requirements given in the plan.** |

After reviewing your test plan results (P7) and applying the changes that the reviewers have given (P8), you made changes to enhance the protection of your IT system/Pc. Show evidence how it enhanced your protection, show the changes with screenshots.

## Changes Based on Client Feedback

## Updated Test Number 9

Graphical user interface, text, application, email

Description automatically generated

The computers password can now expire. As I mentioned earlier this positively impacts the security of the system as it prevents further damage of a data breach. If someone somehow got access to a user’s password, they can’t gain access with it forever as it will eventually expire or will already be expired.

## Updated Test Number 10Graphical user interface, text, application Description automatically generated

The user now has to set a password with a minimum of 8 characters. This makes them more complex and harder to guess reducing the chance of them being brute forced.

## Updated Test Number 11

Graphical user interface, text, application, email

Description automatically generated

The complexity requirements are now enabled on this machine. The User’s password becomes almost impossible to guess and it makes it take a lot longer for hackers to crack since there’s additional characters included.

# Part 4

**D2: Evaluate the plan and the effectiveness of the protected IT system against requirements.**

(Max Word count 600)

*How well did your plan and implementation of the security measure protect the system and meet the requirements?*

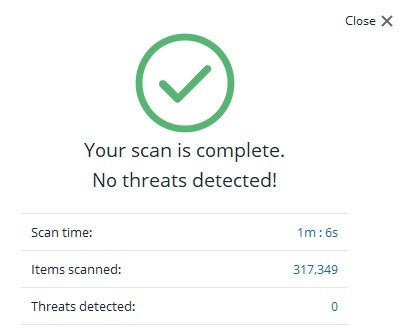
*How well is the system protected?*

## D2 Overall Effectiveness of the Plan

After reviewing the overall effectiveness of the plan after I made some changes, I didn’t notice a massive change. I think this is because I already included the main security in the initial plan. Techniques like WPA2, Software firewalls, antivirus and file permissions make up most of the security on their own. Anything else just adds to their impact.

### How Anti-Virus software impacted the systems security

This was the main method of security that I think made the most impact. This is because Anti-Viruses are very versatile in the forms of security that It offers. One of its main features that I felt best suited the client’s requirements was the background virus scans. With the client being a small business, its going to be harder to recover from malicious attacks. If the anti-virus is scanning the computer daily, it can catch any viruses and alert the user before they spread and cause further harm.



### How WPA2 impacted the systems security

WPA2 is pretty much required for any modern computer system that needs internet access. The use of WPA2 meant that my Wi-Fi connection was secured by a strong password meaning the user could be re-assured that they were protected when using the internet. In the client’s case their business could sends data and it would be encrypted so nobody could spy on it. When the WPA2 was enabled, no Wi-Fi security issues were found.

Graphical user interface, application, Teams

Description automatically generated

### How Software Firewalls impacted the systems security

Speaking of internet security, another reason for the plan’s success was down to the firewall. Having a tool that monitors network traffic in the background is extremely useful. This is because the client’s business may not have the staff to have someone to constantly monitor traffic. When the firewall was set up, no networking vulnerabilities were found.

Graphical user interface, application

Description automatically generatedTo conclude this evaluation, the feedback and the changes made had little impact on the overall plan since the main security techniques I included already met the client’s requirements and business needs enough.

**D3: Demonstrate individual responsibility and effective self-management in the planning and protection of an IT system.**

(Max Word count 600)

*Do an evaluation of your performance in this assignment in relation to taking individual responsibility, Creativity and Time management.*

## D3 Evidence of Individual Responsibility

My behaviour in this project made a good impact on how well it went. I split each task up to focus on them. I was also very co-operative with the client which sped up the time it took to complete each task. I also learned some skills along the way that can help me in the future. I learned skills like:

Time management – this was needed so I could set each task a certain deadline to meet the client’s need.

Online communication skills – these were needed to keep a level of professionalism when talking to the client via email

Critical thinking – this was needed so I could take feedback critically rather than personally to better my security plans and make changes

Windows security soft skills – these were needed to place each security method in a scenario to determine how effective they were.

­General Shortcuts – these were needed improve the speed of certain processes during the project. Examples include: CTRL + C for copy, CTRL + V for paste, WIN + SHIFT + S for snipping tool.

