

Network Security Plan

William Pascoe

CYB-230 Operating Systems Security

Jeremy Cheeseborough

December 9, 2025

Network Security Plan

As a consultant hired by Helios Health Insurance, I was tasked with reviewing the organization's security plans and reporting on my findings. There are many discrepancies in the plan that need to be addressed. AS it shows in the plan concerning potential impact, I believe that the confidentiality of the network falls into the high impact column which states "The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." The reason for this evaluation relates to the use of unencrypted hard drives and an FTP server that uses default admin accounts.

The use of unencrypted hard drives may allow for somewhat faster performance but can be a costly security measure. In the event that someone misplaces a laptop or a malicious person is able to gain access to a desktop, not having any of the systems data encrypted means that any client data stored on that computer is now at risk of being stolen. To remediate this problem Windows Pro has a standard installed program called BitLocker. This program will encrypt the computer hard drives and without a password can only be accessed with a passkey. This passkey is stored off the computer so any attempts to hack the device will result in the data being blocked and unreadable to the would-be hacker (Microsoft, 2024).

The next deficiency that I would like to address is the FTP file server using default admin accounts. The issue with this is the default accounts of most software sold on the market are well known. Anyone can search for these accounts and see what the default passwords for them are (CISA, 2016). If this account is still in existence a malicious person can easily gain access to the file server and have access to the data that it contains. To fix this problem it is recommended that

all accounts have a unique account name and passphrase of sufficient length to prevent being exploited easily. It is also recommended that these passwords be changed on a somewhat frequent basis to prevent being comprised in the event of a data breach.

As security issues are patched and implemented Helios Health will become a much more secure network that will comply with regulations such as HIPAA and others that are needed to ensure public safety and prevent data breaches. Encrypting hard drives and creating unique admin accounts and passwords is a start to getting the system on this right path.

References:

Microsoft. (2024, June 18). *BitLocker overview - Windows Security*. Microsoft Learn.

<https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/>

CISA. (2016, October 7). *Risks of Default Passwords on the Internet* | CISA. Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/news-events/alerts/2013/06/24/risks-default-passwords-internet>