**CYB 230 Project Three**

Douglas Few

Southern New Hampshire University

October 17, 2021

This assessment of the Helios Health Insurance network model will examine both hardware-based and software-based deficiencies through the lens of confidentiality. Upon identifying deficiencies, this report will also attempt to recommend possible solutions that could be pursued in the interest of solving the deficiencies and/or closing any potential holes in the security of the Helios Health Insurance network.

Hardware-Based Deficiency

When it comes to network security, one hardware-based deficiency that was recognized nearly immediately was the fact that hard drives are left unencrypted for the sake of faster performance. While this the availability portion of the CIA triad by ensuring that files are more quickly readily available to those with the authorization to view them, it compromises both the confidentiality and integrity portions by making it easier for those without authorization to view and make changes to the files. The recommended solution is to grant access to folders and hard drives on the network based on the principle of least privilege. This would ensure that only those employees who need access to certain files in order to complete their job functions would be able to access them. While availability may be slightly affected by encrypting folders and hard drives, the protection that comes from it more than makes up for it.

Another deficiency that was identified was the topology of subnets on the network. Each subnet adheres to a bus topology, which causes a number of issues. The biggest issue caused is the fact that every device on a subnet with a bus topology is capable of seeing the activity of the other devices (AfterAcademy, 2021). Once a message is sent from one device, every device on the subnet is made aware of the message, but only the device meant to receive the message is able to accept it. If the message were to be intercepted by another device on the subnet, however, confidentiality would be compromised. The recommended solution to this deficiency is to switch to a star topology. With this topology, each device would be connected to a central node, rather than to each other. This would improve confidentiality overall by ensuring that no other device on a subnet would be able to view the activity of other devices.

Software-Based Deficiency

When examining the software aspects of the network, another red flag was identified almost immediately. End user devices have full access to the internet and are not patched or updated regularly (McAfee, 2021). This poses a serious security risk, as this allows the possibility for end users to visit unregulated websites or download untrustworthy files. Alongside this, there is open access to the WIFI network as well. Both of these factors can impact the confidentiality of the Helios Health Insurance in a major way. Due to the sensitive nature of the information handled in this company, it is imperative that every step is taken to make sure that information remains confidential and untampered with. All it would take to compromise the security of the network is for an end user to download one untrustworthy file. Due to the fact that the computers are not regularly updated, if the file downloaded happened to contain a virus or malware of some kind, it can not be guaranteed that the antivirus software installed would catch it.

The recommended solution to this deficiency is two-fold: set restrictions on internet usage and automate updates. By setting restrictions on web activity, the possibility of an end user’s computer becoming infected with malware or a virus becomes significantly reduced. The system administrator should block most websites on the end user subnet that are not related to business operations. In the event that malware ends up on an end user device, the regularly updated antivirus software should be capable of identifying it at that point (McAfee, 2021). Similarly, WIFI should not be connected to the main network and should be configured so that only employees and authorized guests can use it (Norton, 2018). This would eliminate the possibility of an outside user gaining unauthorized access to the network.

References

AfterAcademy. (2021). *What is network topology and types of network topology?* AfterAcademy. Retrieved October 17, 2021, from https://afteracademy.com/blog/what-is-network-topology-and-types-of-network-topology.

McAfee. (2021, September 7). *Why software updates are so important*. McAfee Blogs. Retrieved October 18, 2021, from https://www.mcafee.com/blogs/internet-security/software-updates-important/.

Norton. (2018, May 26). *The risks of public Wi-Fi*. Norton.com. Retrieved October 18, 2021, from https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html.