Assignment 2 - Evolution 1 - Assessing Networking and Cybersecurity

## Aspects of Developing a Portfolio of What you’ve Accomplished

What do you know - Explore the competencies, skills, and knowledge where you feel you are the most confident and proficient.

My competencies, skills, and knowledge have been based on the many years of working in the IT field and first-hand application of security patches, network management, and group policy management. I have been able to perfect these skills on an everyday basis to learn and grow, as well as keeping up with the current policies and procedures through security patches to prevent vulnerabilities on a network or infrastructure.

Where are you weak - Explore the competencies, skills, and knowledge where you feel you are the lest confident and proficient.

I would have to say my biggest weakness is two different things: the vastness of the entire cybersecurity/network scope required for the healthcare IT infrastructure of the specific devices, and my current knowledge of the requirements of said healthcare IT standards.

Devices being permitted in the segmentation would need to be discussed in a more administrative meeting, what can be monitored according to HIPPA guidelines but still held securely according to the NIST framework the segmentation could be based off. There would need to be a comprehensive understanding for how artificial intelligence could monitor the segmentation tunnel, and if there would be any violation of HIPPA protocol on patient records or what manufacturer of the AI model would be implemented. My best guess would be any kind of AI that is already being used in a government setting, such as Microsoft’s Bing or Co-Pilot.

I am also the least proficient in the understanding of IT Healthcare infrastructure. This comes from my original bachelor’s degree not being IT related, or lack of specifically focused IT in Healthcare classes. I have been able to work with previous MSPs with healthcare providers, but I have never been in the forefront of policies and procedures thereof and how they are implemented.

Future - What do you wish you knew and/or don't realize you are missing

When it comes to the future in cybersecurity, everyone wishes they knew what flaws were in their hardware and software before someone else finds them for nefarious purposes. The vast world of IT and its cybersecurity department is a vast world of the unknown; there’s always something new to learn that you didn’t know before and there will always be something else you don’t know. I wish I knew more about security patches and network management as I’ve held positions that don’t necessarily have that in the job function, so I haven’t been able to exercise or build upon those skills to further my knowledge on them. There’s always something I don’t know, especially when it comes to policy and procedure in the “Why” aspect.

## Contribution Towards the Capstone

Why Networking and Cybersecurity is integrable with the other areas

The networking and cybersecurity is integrable with Data Analytics and Data Management because it monitors what is being permitted to pass through the network in traffic and communications.

How Networking and Cybersecurity is integrable with the other areas

Cybersecurity is important in an IT Healthcare environment to comply with patient privacy according to HIPPA guidelines and to keep confidentiality through security management, and Networking is integrable by creating a segmentation of permitted devices to access specific information without anyone from the outside to gain access to the tunnel.

How Networking and Cybersecurity is integrable with your prior work

I have been grateful enough to have had opportunities outside of the classroom to further develop my networking and cybersecurity skills in my everyday jobs. One of my greatest experiences in the field was working as an Information Systems Security Officer intern with the National Nuclear Security Agency at the Pantex Plant. There, I learn the basics of following NIST guidelines and creating Baseline and Risk Assessments for all sorts of hardware and software for permissions of implementation in the cyber environment and what would need to be changed, altered, or not allowed for it to pass regulation. Following the same NIST guidelines in this project can help lock down and strengthen the cybersecurity of the network that hosts the IT Healthcare infrastructure for this project, and having prior work with it will help create the base understanding for what is needed on the prototype.