**Final Project Part 2:**

**Professional Significance:**

Cyber security is extremely critical in today’s technological world. I firmly believe that every person will need some sort of digitalized protection, now and in the future. I enjoy finding vulnerabilities and conducting investigations of suspicious circumstances. I personally have conducted investigations for several companies that were bound to the payment card industry data security standard or PCI-DSS. The investigations covered flaws in c-store point-of-sale systems, card site devices, and various skimming techniques used on fuel dispensers utilizing various data transfer techniques.

The practice of PCI-DSS is to protect the user’s personal account numbers or PAN. This will allow consumers to have a secure and safe environment to conduct financial purchases. The practice of cyber security isn’t limited to these examples, and reaches a broad range of topics such as phone, computer, network, and even children’s toys. I project the cyber security industries future will be a necessity to protect ones way of life, not just privacy.

The best way to prepare for a role in the cyber security field is to first understand physical security. I served in the military as a Security Forces member for several years, providing various physical security implantations. Cyber security will always encompass physical security, like keeping an entry access log for data centers or critical network infrastructure areas. The next step I would strive to achieve is to hone ones interpersonal skills like effective listening and communicating techniques. I would then progress to the basics in varies computer system technologies followed up with a good old shot of networking and cyber security fundamentals.

**Professional Reflection:**

My main industry focus is in the field of cyber security. I have determined my motivation for this focus based on work experience. When investigating potential cybercrimes I get excited and feel determined to expose the truth. My secondary field of focus is the IOT, in order to be competent in cyber security one must be familiar with a vast array of computer powered devices. This course allowed me to expand my knowledge of relations between all computer science professions. I also feel that I added to my problem solving toolbox by focusing on the minute details that are often overlooked.

In the future, I plan to express my competency in certain areas of cyber security by pursuing industrial level certifications. However, my main goal is to finish my bachelor’s degree in software development. I want to become an extremely well-rounded cyber security professional and in order to accomplish this task, programming is a must know topic. I also need to develop a portfolio and publish its contents to the web, so I can present my knowledge to future employers.

The comprehension of data structures and algorithms are vital in all areas of cyber security. Algorithms are the methods one designs to approach a problem and each individual component of that problem. The various data structures represent the confines or parameters of the software language you are dealing with. In reality, if you can break down malicious software in its simplest form, you can deliver an effective strategy in defending the end users. You can also see a glimpse inside of the criminal’s methodologies and strategies used in cybercrimes. This could potentially be used to construct a signature based on ones use of data structures in algorithms. If you incorporate these signatures in your defense strategy then ultimately you are providing a more secure environment for the end user.