Assignment 1

William Nash

A career in cybersecurity can lead to a large spectrum of jobs and the people in those positions have a different definition of cybersecurity, find different parts of their career interesting, and have the needed skills to be successful in their position. They have all had different experiences that shaped their definition, and perspective on their career through cybersecurity. I will talk about what cybersecurity means for me, some of the interesting and challenging parts, the skills I have that I think will help me be successful, and what experiences help shape my definition of cybersecurity

Cybersecurity at the most basic level is securing digital assets, like emails, passwords, or documents. To me, cybersecurity has two main areas, protecting attacking. Protecting is the idea of securing a system from an attacker, which could mean reducing attack surface, training users not to click on suspicious emails, to having users reset passwords every 90 days. Attacking is the idea of ethical, and when asked, attacking a system to see if there is a vulnerability that could be exploited by malicious users. That could involve social engineering, to brute force password attacks. But the term cybersecurity is ever-changing, every day more vulnerabilities are discovered, more data than ever before is put on cloud storage, more people are using worse passwords, AI like ChatGPT becoming ever more present, and the definition of cybersecurity will continue to evolve.

I think some of the more interesting parts of a career in cybersecurity revolve around protecting and creating, rather than attacking and hacking. During my current job with John Deere, I helped create tools to protect Deere's cloud and I loved it. I loved going from an idea to a finished product and thinking about how our users are going to interact, or how our users might try and bypass our rules. Another interesting part of this career is the blue team side of things. Blue team refers to the process of protecting a system, where then the red team tries to break in. Blue team is interesting because you must think about everything and if you forget something you might leave a hole for the red team.

One thing I think will be challenging for me is hacking. Don't get me wrong, hacking is cool and the thought process behind it is incredible. But I have never been able to look at a system and figure out what the next step would be. With creating software there is only a handful of options a user can do, but with trying to attack a system there are thousands of routes to take. Another thing that makes attacking hard, is the time needed. A penetration test could take months to finish and need a thorough and detailed write-up that anyone could read, and I would just lose interest, and struggle to get the motivation to continue.

I think the biggest skill that will help me is how quickly I can pick up on a new tool, software, or process. I have always been able to quickly pick up and learn new tools, and coding languages as long as I have the drive needed.

I think another skill that has helped me is how self-motivated I can get. I am taking Coms 309, where we have to use a web framework called Spring boot. I started trying to create experiments to learn about Spring boot, and where most of the other students haven't looked at it yet, I have a very basic API setup.

Another skill I have is I don't give up easily. I will continue to try even if I have failed. Now it might take me a second to get back up and start again, but I will always keep trying. I have tried about 5 times now to make a personal website, each try has ended with various problems. I might take a break, and learn or try something else, but I always come back. With a fresh mindset and drive to try again.

Something that has changed my thought and perspective on a career in cybersecurity is working for John Deere. I have had a job at John Deere for just over a year now, on their Cloud Controls team, where I work to make software to protect Deere's Cloud environment. I learned I care less about attacking a system, and more about creating software to help make sure other people follow good security practices. Another example that has changed my thought, is recently I create a simple NodeJS website. It is very simple but has a login system, an access control system, and a SQL database. As part of the login process, I wrote a SQL query that gets the username and password from the user. The way I constructed the query allowed for a SQL injection to happen. I always knew about SQL injection but never understood how a site became vulnerable to it. My understanding of how a vulnerability can be created changed and instead of it being one rooted in the laziness of the developer it changed to be more understanding and that even a good developer can make a simple mistake. It also helped a bit with my confidence in making a mistake

A career in cybersecurity will never be easy, with the many different routes the career can take you, the everchanging definition, and the list of needed skills growing. I think with my current skill set, and skill I will learn. My understanding of what will be challenging for me, and what I will find the most interesting. I think I will be able to have a successful and enjoyable experience and career in cybersecurity.