Reflective Essay

Zakiria Jordan

Old Dominion University

IDS 493

Dr Gordon- Phan

December 8, 2025

I have really learned quite a bit with regard to how technology actually affects the individual, organizations, and society in taking all of the courses that comprise my major in cybersecurity. When I first started looking at my assignments I really thought that cybersecurity was only about computers and finding out who the hackers were. Now that I have written these articles and researched so many subjects, I find out that cybersecurity is more than just a concept; it plays an important role in the way people communicate, the way businesses protect information, and how private data can remain private. In my reflection, I will talk about how my three academic assignments contributed to my development, the skills I learned, and how these skills are going to help me later on in life.

My first assignment was on the social effects of technical cybersecurity systems. Working on this, I was really surprised at just how involved the internet is in everyday life: talking to friends online, shopping online, storing personal information online-without so much as a second thought. Cybersecurity protects that. It keeps our information safe and prevents people from stealing, spying, or otherwise misusing our data. Where I previously understood that cybersecurity was important, I had not grasped how important it was in a social manner. Now I do.

That first assignment also showed me how cybersecurity can affect businesses. Small businesses, especially, struggle a lot since they may not have enough money or knowledge to protect themselves. I learned that even one small mistake in security can make a business lose money, customers, and even trusts. That is actually when I seen that the need for employee training, contingency plans, and budgeting for security equipment was very important. Cybersecurity does not start after an attack has already happened so preparation is needed beforehand. The earlier companies start to get ready, the easier it will be for them to survive such attacks.

I also learned about cyber threats such as hacking. I learned of black hat hackers, who break into systems for their personal gain, and the white hat hackers who actually try to fix the security problems. That taught me that cybersecurity is ever on the move. The hackers do not stop learning; hence, defenders should never stop learning either. Simple habits such as updating your software and keeping strong passwords make all the difference. Writing on this actually changed my thinking whenever I went online. Now I understand that anyone can become a target online, so everyone needs to be on guard.

My second academic work was on the breach of data on Facebook. Before I had looked into this topic, I had heard about data breaches but didn't know exactly how they went down. Learning about this case taught me just how hazardous weak security can be. More than 530 million users had their personal information exposed because of poorly protected third-party apps and weak password storage. That just made me realize huge companies are not always as secure as we think. A single mistake in a system may expose millions.

This paper also helped me understand why companies should be held accountable when they fail to protect users accordingly. Facebook was fined millions of dollars and received a lot of backlash from the public. A lot of its users had become quite distrustful of the company. Something that I also learned was that cybersecurity is not just about technology, but it is also about law, accountability, and ethics. If companies do not respect user privacy, something must happen. That taught me that security is more about protection; it is about honesty, responsibility, and fairness.

The third academic paper was about Meta and privacy through the perspective of a Kantian ethics approach. This assignment helped me understand the moral side of cybersecurity. Using Kantian ethics, I understood that companies should treat users as human beings with dignity. They shall not design systems that fool people into doing something or show private information without warning. It turns out that Meta

failed to do so because users could share private information publicly without knowing. This was particularly instructive to understand the harm that can come from creating technology in a way that does not take user protection into account.

The lesson of Kantian ethics is that morally right actions show respect for persons and their privacy. If a company prioritizes engagement over users' safety, it is treating them as a means to an end rather than as human beings. This changed my perspective on software design and technology development: cybersecurity professionals are responsible for building not only safe systems but also ethical ones-privacy is a right, not a luxury.

Looking back at all my assignments, I could see the major skills I developed. First was research. For each paper, I had to look up sources, compare information, verify facts, and understand new ideas. Research helped me learn deeply instead of just memorizing. It also helped me break down complex information into something I could explain clearly. This research will continue to help me with cybersecurity because the field moves quickly, and new threats pop up every day. Being able to research means being able to stay informed and adapt.

The second skill developed was Linux skills. Learning how to use Linux taught me how a computer works and behind the scenes. I learned how to move through things like commands, manage files, and understand permissions in general. Linux is important in cybersecurity, so it makes this skill count for technical work. I am still learning and trying to get better at using this but even the basics gave me confidence. Linux taught me to solve problems step by step, think logically, and deal with challenges without giving up.

The third skill I perfected was academic writing. Writing taught me how to organize my different ideas, explain concepts clearly, and effectively communicate. It showed me how to create arguments,

support these with facts, and focus on writing with purpose. Good writing makes a big difference in cybersecurity since professionals often have to report on threats, write policies, explain risks, and communicate with teams. Clear writing will not cause any confusion but rather build trust and keep people informed.

In conclusion, my academic work gave me a completely different and personal understanding of cybersecurity. I learned about how technology affects society, how security failures have impacts on millions of people, and how ethics shape the way systems should be designed. After many courses I developed good research, Linux, and academic writing skills. I'm still currently trying to figure out what I would like to do after I graduate but I would say I have good skills so that I would be comfortable in a lot of positions that I'm looking at. Therefore, I will continue to perfect my craft so that I'm ready to step up to any plate that I'm given.