Michael Becker

Professor Franklin

CYB E 234

May 7, 2024

Final Term Paper

This semester has been full of many interesting topics and has brought to light many different thoughts and ideas that will change my thought process as I eventually graduate and enter the cybersecurity workforce. CYBE 234, the class on legal, professional, and ethical issues in cyber systems, taught precisely that. Over the past semester, my understanding of cybersecurity has evolved. To be more specific, through lectures, discussions, and personal reflection through assignments, I've learned to appreciate the true power of cybersecurity. Cybersecurity isn't just "computer work" and protecting information; it is composed of complex ethical and moral decisions. This essay will cover some of the most influential topics I learned in class and how those have challenged my initial thoughts. It will also cover the necessary soft skills for my career and what I believe I will struggle with in the future. Overall, this class has prepared me with the ethical tools to deal with many different problems that I could face in the future.

Coming into this semester, my knowledge of the importance of ethics within cybersecurity could have been improved. Before taking a deeper dive into class and the material involved, the main factors that guided my ethical decision-making were transparency, integrity, and social responsibility. Without knowing the full extent of ethical frameworks and viewpoints within the cybersecurity field, I still had my ethical guidelines that apply to life in general. Before entering class I assumed that these moral guidelines I set for myself to deal with future

problems in my career ultimately would be satisfactory. I am an ethical honest person wanting to do the right thing in all scenarios. If I were to be faced with a problem, I would solve it to the best of my knowledge and in the fairest way. But what are the most important factors that will decide my ethical decision making? This appears to be a simple question, and at this point in my school career, after taking CYB E 234, my main factors have remained the same. As a cybersecurity professional I should have a respect for privacy, integrity, accountability, legal compliance, fairness, risk management, and an understanding of how consequences will affect the people around me. Ethical decision-making does not need to be a hyper-complex analysis of problems, and most of it should come with experience dealing with problems. That being said, how has this class affected my understanding of my minimalistic view of an ethical framework to guide myself into a cybersecurity career in the future?

The class discussions and information brought to light in this class have significantly changed how I view issues. In the first week of class, lecture two referenced the topic of security. To be more specific, the lecture states that security is about trade-offs, and you cannot obtain privacy without security, but security can be increased by a decrease in privacy. This was my first introduction to the complex concepts that would be up for discussion later on in the semester. A concept like this is crucial for cybersecurity professionals to understand and be able to gauge. Yet, these questions don't necessarily change my frameworks but it does change how I use the framework I set for myself. I have to weigh out the issue and the consequences to determine an answer to a problem. The other central theme that I have seen throughout this class is that there is no real answer to any moral question.

This theme can be represented in many lectures. Throughout this semester, there has been a multitude of discussions that have somewhat proven that there is no cut-and-dry answer to any

issue. For example, in lecture three, the discussion question posed referred to a runaway trolley, and you have the decision to pull the switch and kill one person by changing the direction of the train or do nothing and kill five people. In lecture seven, the class discussion revolves around having a job at a small software startup and having to decide to be honest with your customers with the ultimate risk of having the startup go under. These are just two examples of the many that have changed my perspective on the problems that reside in the field of cybersecurity. There is no clear black and white, right and wrong, in these discussions, and that proves the theme of "no real answers." The questions in class may not be direct problems that will be faced in cybersecurity, but they represent a complex issue with multiple factors. The understanding that I've gained from these class discussions is fundamental due to the fact that it allowed me to view problems not as right or wrong but as getting the best outcome using my ethical framework. These discussions were a great way to analyze the differences in your thought processes throughout the course. The class also introduced many different ethical viewpoints and thought processes that needed to be analyzed in multiple writing assignments. Due to the deep dive into these viewpoints, they are another important part of the class that has made me think about cybersecurity and the potential issues differently.

Lectures three through seven introduced many different ethical frameworks that have challenged my thinking. As much as I learned, it was also a great indicator of what category I mostly fall into when analyzing my own ethical framework and what I value against those of many others. The Utilitarian, Kantian, Virtue, and Consequentialist perspectives help create a good guideline when analyzing information and issues. In these lectures I have learned that the Utilitarian approach emphasizes actions that would maximize overall happiness or well-being. Kantian ethics is more morality-based, specifically referring to a moral duty, principles, and the

intrinsic moral value of actions. In this perspective, the outcome measured isn't considered nearly as much as in the Utilitarian perspective. Learning about ethical frameworks was very important. It gives you more to consider when thinking of problems you could potentially face. From lecture five I have learned that Kantian ethics is deeply rooted in logic. The creator, Immanuel Kant, proposed the CI (categorical imperative), which is a universal moral law that applies to all rational people. He suggested that immoral actions are, therefore, irrational because they violate the CI. The lecture also taught me about how Kantian ethics emphasizes the importance of duty and moral obligation within ethical decision-making. The Virtue ethics perspective emphasizes moral character and virtues. The Consequentialist approach, introduced in lecture six, revolved around doing something because it is who you are as a person as opposed to because you are supposed to. It focuses on practical reasoning and, like Utilitarianism maximizing good while focusing on the outcomes of a situation. Although simply learning about these perspectives did slightly change my thought process, they only truly changed my perspective when they needed to be applied. The writing assignments in this class had very open-ended prompts, which allowed for a lot of thinking and analysis. An example of this is assignment two where we analyzed ethics versus morals and had to create a scenario where either ethics or morals would take precedence. In this assignment you had to apply the ethical and moral frameworks we have learned, as well as think of scenarios in the cybersecurity field. This changed how I thought about many problems I might face throughout my career. Through these exercises, I learned the importance of ethics in the field and realized that simply being a "good" person and doing the right thing won't necessarily cut it. Coming into this class, I believed that ethics weren't a problem and that learning about different frameworks wouldn't benefit my future career. But after the application to different scenarios through in-class

discussions or assignments that thought has changed drastically. I realized that one ethical framework or train of thought usually isn't the right answer. No one should analyze a problem over a single approach. It should be a mixture of the information you have as well as your own personal thoughts. So, the ethical dilemmas and frameworks that we have learned in class allowed me to pick out what I lean towards, and that has been a mixture. There are some scenarios where maximum happiness is the "right" answer, and there are some cases where it's not. There are some problems where Kantian ethics produces a more logically sound answer to a problem than the others. The main takeaway from this part of the class was that there is no "right" answer, there is only a good guess. The class has taught me much about how to manage problems in the realm of cybersecurity and another important aspect that comes with the Ethical OS.

This class focuses on the ethics within the cybersecurity field, and that is important. But what is even more important for students is learning about the potential dangers that lurk within the field. It is important to understand the field of cybersecurity on a higher level as well as just technology. The Ethical OS, introduced in lecture four, is a framework due to the fact that ethics can be a risk issue. It has to be understood that risks cannot only come from outside sources but in the production of an app or software, or any piece of technology, you can create risks for others. We still need to limit those risks, and thus, the Ethical OS is given to us. This was a big turning point in my thought process of cybersecurity. I have been in Aerospace engineering up until this year and picked cybersecurity because I think it is a very important job protecting people's information. The introduction of the Ethical OS and its application on the mid-term assignment really changed my perspective and helped me evolve as a cybersecurity student. This is another major factor that will help me with my ethical decision-making in the cybersecurity

field. As I've said before, I had a very loose framework on ethics coming into class, and I don't think that has changed, but how I apply it to situations changes drastically with each step further I take into the field. The Ethical OS outlines a framework of risk zones, some of them being "Truth, Disinformation, Propaganda," or "Hateful & Criminal Actors." Pairing the new knowledge of the Ethical OS with the prompt for our mid-term assignment analyzing the concept of Twitter helped me rewire my brain to a point that allowed me to see different things in companies. The mid-term assignment was another very good representation of how the class as a whole gives you tools and then makes you use them in the assignments. Although there was no real "technical" problem-solving in this class, the tools that the class gears you with throughout the semester have made me believe that my ethical decision-making is constantly evolving, and If I have a good base, I can solve any issue as long as I learn the specific tools to deal with them. The Ethical OS is just another tool in the cybersecurity realm that you can use to help solve a problem more easily, but it doesn't change my ethical decision-making base values or factors. It just changes how I perceive problems.

My most important factors in ethical decision-making revolve around respect for privacy, integrity, accountability, legal compliance, fairness, risk management, and an understanding of how consequences will affect the people around me. My ethical framework started off with trying to be a good, honest person, but throughout the class, I have learned more and more about the field and, in the end, have added a couple of things. Before coming into this class, I didn't think it would be as much about soft skills as it is, and with that, there are a couple of soft skills that will be important to my career in the future.

In lecture twenty-six, the idea of professional and business ethics is introduced. It explains different codes of ethics, such as the ISC2, which states to "act honorably, honestly,

justly, responsibly, and legally." In the business world, I hope to get a high-paying job with which I feel satisfied. This is the most basic answer, but it is the truth. There are many soft skills that I believe are lacking in the industry, which are accountability, critical thinking, professional competence, and communication. The realm of cybersecurity is constantly changing and I feel it to be very important to keep up with current threat mitigation tactics or tools or new technology. I also believe critical thinking to be important when adhering to an ethical code and solving problems. Accountability is another soft skill that I believe will be respected in the future if mistakes are to be made when trying to resolve a problem. Last of all, communication is key in most jobs, you have to be able to clearly and concisely express your thoughts and ideas while remaining respectful. Now, the struggles I will most likely face come on the technical side. I believe many soft skills to be my strong suit. I would like to say that soft skills will help carry me farther into the field, but where I believe I'll struggle is the technical side. I have been doing well in classes revolving around cybersecurity, but as for learning new technologies quickly, I don't know if I would be able to keep up as fast as others. I have stated that some of the soft skills that are important for my career in the future are professional competence and keeping up with the latest techniques and tools. I think I'll struggle with this due to the fact that I tend to need more time to learn compared to my classmates around me. But in this stage, I am driven to be successful and would create a time slot each day to learn new things relevant to my job or career path. Another way I could cope with these strategies is to seek mentorship. Obviously, I'm not going to be the CEO of a company out of college and will start very low in the corporate world of cybersecurity. I could turn my weakness of technical skills and turn it into a positive by seeking out people who know more and simply ask questions. I not only get to learn but will be seen as having a thirst for learning and education whilst also showing interest.

Last of all, if there is one thing that this class has taught me, it is that cybersecurity is way more complex than previously thought. This class has made me excited to step into new classes, gain new ideas, and learn more about the field. I am so happy that this class was a requirement because it only made my thirst for knowledge in the field greater. I have learned a lot this semester and I feel as if I have a pretty good ethical framework. Although I am nowhere near ready to enter the field, I feel like this class has given me a great path to move on, allowing me to assess my strengths and weaknesses and giving me strategies to help me with my career.