Declan Creadon

Professor Franklin

CPRE 234

May 7th 2024

Final Term Paper

The world of cybersecurity is multi-faceted, and many people have this preconceived notion that cybersecurity is nothing more than some computers and software. Now, at the beginning of the semester, I was one of those people as well. This semester has taught me that cybersecurity is much more than that. Cybersecurity is a complex landscape that requires ethical decision-making at every corner. Is this illegal? Am I breaking any laws? Is what I did right? These are all questions that many cybersecurity professionals ask themselves throughout their careers. Ethical decision-making is a crucial concept in the realm of cybersecurity. Many factors can guide an individual's ethical decision-making. I find integrity, accountability, and confidentiality to be the most critical factors in my decision-making. The factors of ethical decision-making can be different for everyone, and preconceived beliefs such as religion, personal bias, stereotypes, and social influence play a significant role in shaping people's ethical decisions. However, that is not the only force in shaping the factors of ethical decision making. The classroom also plays a significant role. This semester, there have been numerous discussions and case studies that have influenced my understanding. Additionally, many soft skills will be needed in a cybersecurity career to adhere to this ethical code and achieve my goals. In a cybersecurity career, there will be challenges along the way, and I will need to develop strategies to overcome these challenges.

Ethical decision-making is essential in many professions but is highly important in a cybersecurity career. Ethical decision-making is the backbone of cybersecurity. It is needed at every corner, especially if conducting a penetration test. Reflecting on the semester, I am able to recognize what the most important factors in making ethical decisions are.

First, integrity is a foundational factor in ethical decision-making. Upholding honesty and having strong moral principles are two things that are essential in maintaining trust between yourself and others. Integrity is vital because without integrity, there would be little to no trust, and in cybersecurity, trust between you and the organization is one of the most important aspects. Another reason integrity is important is because it plays a massive role in guiding my decisions. Integrity helps me identify the right decision no matter the outcome I face. It helps me realize that the right decision might not always be the most popular decision or the decision with the most impact. Integrity guides me when navigating tough ethical dilemmas, which is why I greatly value it in the ethical decision-making framework.

Secondly, privacy and confidentiality are paramount when making an ethical decision. As a professional, maintaining confidentiality is very important. It fosters a sense of trust within your professional relationships. Adding on, the privacy rights of others should always be of utmost importance when making a decision. There should be no reason as to why you would want to disclose this information. This information should always be respected and protected no matter the decision. Additionally, adherence to legal and ethical standards regarding privacy and confidentiality is needed. This not only upholds professional standards but also promotes a culture of integrity and a respect of privacy. In all, when making an ethical decision, privacy and confidentiality should always be considered. There is no reason to do excess harm to people that are not involved.

Lastly for me, accountability is also a key factor when it comes to navigating an ethical dilemma. Accountability is essential in ensuring that answers are provided for the actions of individuals or organizations. Accountability extends beyond just getting answers; it showcases transparency, honesty in some cases, and integrity in all aspects of the outcome. Now, this accountability can go both ways, which is another reason why I place it so high. Sometimes, your decision may not be the best, and you need to be able to take ownership of the consequences that follow your decision, whether positive or negative. Like with the other two factors, accountability fosters a sense of trust and credibility. Accountability is also suitable for reflection. Taking accountability allows you to reflect on past decisions and identify where you went wrong or where you can improve. Ultimately, accountability is a guiding principle when making ethical decisions and ensures that decision-makers, along with organizations, are held to high standards of conduct.

Preconceived beliefs are a strong force that can affect an individual's ethical decision-making process through bias, stereotypes, and judgments. These beliefs, many of which were formed during someone's upbringing, can significantly impact how an individual navigates an ethical dilemma. Preconceived beliefs may lead individuals to have a bias when it comes to making decisions rather than weighing out all of the possible outcomes. For myself, I have always had a high sense of accountability. Growing up, I was a troublemaker and would get myself into situations where there was no easy way out. When this was the case, the only way out would be to own up to my actions and take accountability. My mom also played a significant role in holding me accountable. She instilled in me to always tell the truth and take accountability whenever necessary because that was always better than lying. So, that is what I always did. Ultimately, accountability has been a crucial part of my upbringing and happens to be very important when making decisions as well. In a cyber security career, I will need to be able to take accountability if something goes wrong or if my decision has a bad outcome. I need to be the guy who can go up and apologize for the things that I have done wrong and be able to look back at my mistakes and better myself for the future.

As said previously, the classroom also has a significant role in shaping how an individual navigates an ethical dilemma. Throughout class this semester, we have looked at and discussed some topics that have helped shape how I view ethical dilemmas. Upon coming into this class I had little to no knowledge about the ethics involved with a cybersecurity career. Something that stood out to me from one of the first discussions was the train dilemma presented for the class. The dilemma was a situation in which a train was coming, and you had a decision to make. You could not touch anything, and the train would kill five people, or you could flip a lever, and the train would kill one person. This dilemma was tough because no matter what, somebody was dying. Ultimately, I decided not to do anything and let fate stay the same. However, this dilemma taught me something essential that will stay with me throughout my career. This dilemma taught me that sometimes, no matter what decision you make, there are always going to be consequences that follow. You could weigh out all of the possible outcomes, and in every one, there is a consequence that will follow. In all, this dilemma taught me an important lesson that will resonate throughout my career. It taught me that there are always consequences to your decisions, whether they be good or bad.

Another important topic we covered in a lecture that helped me shape the factors for the ethical decision-making process was looking at the CIA triad. As mentioned before, coming into this class, I had no idea about ethics in the realm of a cybersecurity career, so the CIA triad was completely new to me upon seeing it for the first time. I remember from the lecture that we were presented with the three pillars of the triad which are as follows: confidentiality, integrity, and availability. After discussing these three pillars, I realized the importance they could carry in a cybersecurity career. These three pillars are the framework that all cybersecurity professionals should follow to ensure they navigate situations ethically. Confidentiality and integrity were the two that stood out to me the most. In this discussion, I learned things such as privacy rights that, if infringed on, could carry some serious consequences. I also learned that upholding confidentiality maintains trust as a whole between you and the company. Additionally, we discussed the importance of integrity. Integrity is essential when making a decision. Integrity ensures that the decision is honest, unbiased and the best decision possible. Overall, the classroom has impacted how I view ethical dilemmas and a career in cybersecurity. It taught me that ethical dilemmas are a vital part of a career in cybersecurity. It also taught me the two critical factors of confidentiality and integrity. These two factors should be incorporated into any ethical decision that is made. They ensure you are not breaking any rules and are making the best decision possible.

In a cybersecurity career, there are going to be soft skills that are necessary to achieve your goals. My goals are simple. They are to start with a company that will train and develop me for the more complex things in this field. After this, I plan on becoming the CISO of a company. That should be the end goal for everyone in cybersecurity. It is the highest position that is attainable in a cybersecurity career. In order to achieve these goals, an essential soft skill is adaptability. Adaptability is prevalent in a field such as cybersecurity because it is ever-changing. Every day there are new exploits and vulnerabilities that need to be fixed. Adapting is just part of the job in a cybersecurity career. According to softsideofcyber.com, “Adaptability is a person's ability to be flexible and adjust to the changing circumstances in their environment.

Information Technology and cybersecurity are constantly evolving which makes your ability to adapt to those changes extremely important" (Domizio). As you can see, adaptability is a key aspect of a career in cybersecurity and is very important in achieving my career goals. If I cannot adapt to the complex landscape of cybersecurity, my goals will never be achieved. That is the whole basis of cybersecurity: the ability to adapt. Adaptability is necessary if I want to be successful in this field and achieve my goals.

Now, another soft skill that will be necessary in a cybersecurity career is communication. Effective communication is essential in any career but is of utmost importance in a cybersecurity career. There are many forms of communication, but open-mindedness is a specific, critical form. According to LinkedIn, "open-mindedness is a must-have. There are usually many ways to solve a problem, so look for options that meet key interests. Be willing to listen to different ideas and consider alternative solutions. Stay solution-focused rather than positional" (Raquel). As you can see, communicating with an open mind is essential when making an ethical decision. By communicating with an open mind, you learn about both sides of the decision. By understanding both sides of the decision, you will be able to keep your morals strong and come up with a decision that benefits both parties.

A final soft skill that I find very important in this field is logical thinking and troubleshooting. As a cybersecurity professional, I will encounter many problems; when a problem is discovered, I will have to be able to overcome it logically. According to netsurion.com "Cybersecurity professionals need to have strong analytical and problem-solving skills. They need to be able to analyze problems, find root causes, [and] apply solutions" (Netsurion). It may not seem like it, but logical thinking and problem-solving are essential in ethical decision-making. When faced with an ethical dilemma, thinking about it logically allows me to analyze the situation from both sides and consider all of the various factors that could have contributed to this dilemma. Moreover, problem-solving skills are also just as important. Just like problem-solving, when navigating an ethical dilemma, you will have to overcome challenges to find a solution. Overall, refining these two skills will be beneficial for navigating ethical dilemmas and will continually improve my ability to make a morally strong decision.

In a cybersecurity career, there are going to be many areas where you may struggle. A career in this field is never easy, and the landscape constantly evolves with new cyber threats emerging daily. That takes me to the first area where I may struggle. Keeping up with these threats is more complicated than it looks. The sheer number of possible attacks and infiltration methods are sometimes overwhelming, and new attacks are being added daily. To cope with this challenge, I must stay diligent in recognizing and learning the latest trends and attacks. By doing this, I will be able to patch and mitigate these attacks as quickly as possible. Another area that poses some severe struggle for me is the pressure and stress of being a cybersecurity professional. I struggle to handle pressure and as a cybersecurity professional, there is pressure everywhere. For instance, there could be an attack at any time, day or night, meaning you must be ready to respond at any given time. This could lead to long work days and requires professionals to be prepared to respond to incidents outside of regular work hours. This pressure to remain readily available leads to high levels of stress and an overall decline in mental health. To mitigate this pressure, I must develop strategies to help me with pressure and stress. First off, this can be built with practice. I could put myself into high-pressure situations in order to create a sense of being able to work under pressure. To deal with stress, I will use my downtime to enjoy the little things in life and take my mind off work. This is essential in staying mentally strong and not letting stress overwhelm you. Ultimately, as a cybersecurity professional, I will struggle in some areas, but that’s not what is important. What is important is how I respond to this struggle. I need to be able to develop strategies that will aid me in overcoming these challenges.

In conclusion, this semester has impacted my knowledge of what is involved in a cybersecurity career. If anything, this semester has led me to want to pursue a career in this field further. I learned there is more to this than just sitting at a computer looking for vulnerabilities, attack vectors, etc. It taught me a side of cybersecurity that few people find very important. It showed me that ethics play a crucial role in various aspects of this career and taught me how to be morally strong and come to the "right " decision. This semester has also helped me identify a new career goal. Before this class, I did not even know that a CISO was a position within a company. Now, being a CISO is my long-term goal and something I want to achieve in this career. However, no matter my position, I will be presented with ethical dilemmas. Integrity, confidentiality, and accountability are the three factors that I will need to rely on in order to guide myself through ethical dilemmas. Following these three factors, combined with my preconceived beliefs and what I learned this semester, will ensure that, in the end, I am making the best decision for the dilemma at hand. In the end, as I reflect on the semester, I appreciate all of the things I learned in this class and am grateful for the impact that this class has already had on my cybersecurity career.

Works Cited

B., P. Raquel. “The Power of Communication: Why Soft Skills Matter in Cybersecurity.” *LinkedIn*, 15 June 2023, www.linkedin.com/pulse/power-communication-why-soft-skills-matter-penelope-raquel-bise-#:~:text=Cybersecurity%20is%20a%20complex%20field,find%20the%20best%20path%20forward.

Domizio, Frank. “Adaptability.” *The Soft Side of Cyber*, The Soft Side of Cyber, 19 Jan. 2023, www.softsideofcyber.com/framework-adaptability/.

netsurion. “Eight Essential Skills for Modern Cybersecurity Professionals.” *Netsurion*, www.netsurion.com/articles/8-essential-skills-for-modern-cybersecurity-professionals#:~:text=Logical%20thinking%20and%20troubleshooting%3A%20Cybersecurity,to%20improve%20their%20security%20performance. Accessed 7 May 2024.