Benjamin Hall

Dr. Blakely

CprE 234

May 6th, 2022

When pursuing a career in cybersecurity, one must have a solid set of principles or code of ethics to make consistent decisions in such a field. Through this semester, we learned various ways to assess the morality, ethicality, and legality of various decisions. Through the discussions and lessons I've learned in class, I've developed a more well-thought out and consistent code of ethics for myself to follow in my pursuit of a career in Cybersecurity. The principles in my code of ethics are: protecting the common will, maintaining trustworthiness, humanizing your users, protecting the company, and constantly pursuing advancements in security and privacy.

First and foremost, my most important principle is to choose the option that protects the common will of the people. As a field, cybersecurity at its core is about protecting the security and privacy of the people. Cybersecurity engineers have a duty to always prioritize the common will of the people when making decisions in how we do our job. This is the most clear way to act in the most moral and ethically sound way possible. This aligns with the virtue of beneficence, the virtue of having the people's good will in goal. I talked about beneficence being the most universal and important virtue because I believe it is in human nature as a societal structure to collaborate. We got this far as a species by being able to cooperate together. By putting the common will of the people first, we can advance our benefit towards the general public by doing what this field does; ensuring security and privacy to users. Before I took this class, I had looked at this aspect from a purely utilitarian ethics standpoint; asking what option gives the best to the

majority; and I think this utilitarian logic holds true for the most part until you humanize both sides. Employing utilitarian ethics was always my default beliefs and logic before I had taken this class, but after more introspection and learning of lessons in my class, I learned this code of logic alone cannot support an good, encompassing code of ethics in a career like Cybersecurity, where one is constantly being given difficult dilemmas and problems.

To go along with other principles, another important principle I see in my career in Cybersecurity is maintaining honesty in trust in the public. I talked about fidelity, the virtue of being true and faithful to your word, in my essay about virtues we hold, and this is important to me. A common issue the people have in this day in age is a common lack of trust in big companies, creating a divide between the people and companies. For example, Equifax failed to disclose a massive leak that affected upto millions of Americans. They only disclosed the leak four months later from being notified, when they had noticed a suspicious network on their servers (Schneider & Arnold, 2019). This is a disturbing lack of good security practices and ethics that I plan to uphold in my career in Cybersecurity. On the other hand, companies like Signal exhibit model honesty and trustworthiness. When they were subpoenaed by the US government in 2021, they were honest and explained how their system of encryption and message transfers does not allow them to know who a user is messaging or what they messaged (Ruiz, 2021). Signal is beloved by their customers because they openly discuss how their product is secured and what personal data they have access to. The trust their customers have in them and their product allows them to grow as a company. By always acting in ways that inspire trust, you can create a more honest and transparent environment that helps you grow and incorporate better cybersecurity practices.

Another principle for myself is to treat each user that you are protecting as if you knew them. Oftentimes there is too much separation between a line of text and yourself. Outside of even cybersecurity, many online issues today would be solved if we could fully visualize that there was another human being on the other side of the screen. If we visualize that human being on the other end, it would inspire more sympathy that creates a level of understanding and challenges our actions that we would do. Before doing anything, I try to always ask myself if I would be okay with it if I was on the receiving end. Sometimes I struggle with this principle, as I can be prone to act too soon with poor initial decision making that was made in the spur of the moment. I often make selfish choices that make my life easier, so taking a step back and rethinking about my choices with my code of ethics is something I could develop as a skill in order to be more disciplined with my code of ethics.

Lastly, another principle would be to act to preserve and grow the company. While all the rest of this code is based on morality and ethics, we also have an obligation to protect the company or organization we are being hired by. While if any matters directly conflict multiple other principles, I would most likely side with my other principles first. In most other cases, it's about finding a good medium between cybersecurity and practicality. There might be some best practices that detract too much from the company, either taking too much training or time out of employee's time for the practice to be worth it. For example, having a YubiKey for every employee might be the best practice for the company. However, you would have to purchase Yubikeys for every employee in the company. Beyond that, you also would need to train employees to learn how to properly use the YubiKey for login and security, and potentially pay for additional YubiKeys as it is inevitable that employees will sometimes lose, and additionally

require more action from IT staff to reset the user credentials in whatever User Identification and Authentication system you are using. In practice, this approach is too expensive for the majority of companies. It may not be worth the investment for low-risk companies that do not have to meet strict security guidelines like HIPAA and similar laws to protect citizens in high-risk environments. As a cybersecurity engineer, you have to consider the Opportunity Cost and sometimes go with a compromise between the ideal, best practices for cybersecurity and the more cost-efficient route when implementing security and privacy features.

Another principle to uphold in my personal code of ethics is about always seeking to improve myself and my practices. This principle can best be practiced by exhibiting humility, the virtue of knowing one's importance and worth. I talked about this virtue in my personal virtues essay. Many times, when we learn new things, we initially believe we know everything and grow complacent with our knowledge and skill level. However, it is important to always seek to increase your knowledge set on topics in a field like Cybersecurity. Threat actors are always looking for ways to exploit your weaknesses which requires you to always be up-to-date with the latest technologies and news. I talked a bit about my desire for a constantly changing and challenging field being part of my desire for my career in Essay 1. I believe challenging yourself to do more and taking yourself out of your comfort zone is a fundamental requirement in enjoying life to the fullest. While this is a more selfish reason for my personal code of ethics, I think it is beneficial towards motivating myself towards more morally and ethically sound actions. Going back, this way of method of self-improvement also extends to being complacent in your current practices. I've seen many times companies grow complacent with their current cybersecurity practices and cut corners on their security to save money. These companies may

lay off critical cybersecurity employees or stop paying for important subscriptions towards a well-rounded cybersecurity defense. All these times these companies cost themselves money by incurring cyber attacks that have varying levels of damage. For example, in the earlier case with Equifax, they were sued for up to $70 billion in damages (). If they had simply acknowledged that their software was out-of-date and updated the software, they could have avoided the damages as a result of the data breach. As a skill, challenging yourself and others around you to improve themselves is an essential skill to be competitive in the cybersecurity industry.

Overall, the class has helped me more thoroughly determine my morals and ethics towards Cybersecurity. Being a guardian of the common will, acting in ways that inspire trustworthiness, humanizing and sympathizing with your users, acting to protect the company, and not being complacent and aiming to improve your skills and knowledge about Cybersecurity are the personal code of ethics I've developed through discussion and introspection throughout the semester in this class.

*Works Cited*

Ruiz, D. (2021, April 30). *Signal app insists it's so private it can't provide subpoenaed call data*. Malwarebytes Labs. Retrieved May 6, 2022, from https://blog.malwarebytes.com/privacy-2/2021/04/signal-app-insists-its-so-private-it-cant-provide-subpoenaed-call-data/

Schneider, A., & Arnold, C. (2019, July 22). *Equifax to pay up to $700 million in Data Breach Settlement*. NPR. Retrieved May 6, 2022, from https://www.npr.org/2019/07/22/744050565/equifax-to-pay-up-to-700-million-in-data-breach-settlement