Eric Mung'aũ Preston

04/19/24

PHIL 355E: Cybersecurity Ethics

Dr. Ryan Thompson

Old Dominion University

Reflective Assignment

INTRO

Throughout this cyber ethics class, I've gained much-needed insight into different issues within the cybersecurity industry. Going through each case study has helped me tackle the moral dilemmas within abstract principles, information, business, and different forms of conflict. Yet, while the course has overall been beneficial in gaining a new understanding of the ethics of cybersecurity, three topics stood out the most in impacting my perspective.

TOPIC 1 – CORPORATE SOCIAL RESPONSIBILITY

A key subject for me was the importance of corporate social responsibility (CSR). While I initially had an older perspective of businesses as primarily being for profit, I learned that many more complexities need to be involved and addressed for them to function in the modern day. For example, if information belonging to an organization is breached and severely impacts consumers, the organization is responsible for fixing the issue. Also, to take accountability for jeopardizing their safety. Having a business follow that new model shows a business's awareness to follow through on social responsibilities and understand the potential consequences of their actions. I now know that those social responsibilities are a primary objective for any business and cannot be disregarded for potential or further profit.

The primary application of CSR to an eventual career could be having the public's safety as a top concern. The concern can involve improved preventative measures against attacks, advocating for resources to be spread to other communities that need them, and having transparency with the public to give assurance of dedication to social responsibilities. These actions in the future show a desire for the public's well-being, and that is how I would want my actions to be reflected in my cybersecurity career.

TOPIC 2 - WHISTLEBLOWING

Another topic that I gained a new perspective on was whistleblowing. I previously thought that whistleblowing occurred out of malicious intent. However, after going through the module, I realized that the reasons that cause one to choose to become a whistleblower are much more complex. Whistleblowing by itself is not meant only to be a way to expose an organization for malicious intent. However, while that can happen under the circumstances of a fired employee holding a grudge, other forms of reasoning are out of loyalty to the organization's values and wanting it to improve from its current status or to protect customers or people from being harmed or put at risk. After learning about these different forms of reasoning, my new position is that blowing the whistle on an organization can be an ethical option if no other methods cause change to a harmful status quo.

My takeaway is that I am now more aware of the importance of whistleblowing. I intend to have the topic guide me by being stricter about organizations' adhering to their values and highlighting the different forms of reporting that exist outside of whistleblowing. I plan to advocate for organizations to be accountable for keeping the public's information safe and for reporting methods advertised as an ethical method for change. I also plan to evaluate my

practices to ensure they're ethically sound while working in an organization. This includes proper transparency and reporting breaches to the public to maintain safety.

TOPIC 3 – INFORMATION WARFARE

My final topic of interest was information warfare. Before the module, I didn't consider the ability for warfare to be conducted using social media. While I always knew it could have some effect on people due to the amount and type of content, reading the case study on the 2016 election and the overwhelming ability of algorithms to spread misinformation on a national scale was surprising. Furthermore, multiple parties, from non-state actors to proxy forces influencing the democratic process, showed that while platforms like social media can build connections, that same ability can be used as a weapon to cause chaos. I now know that I am more wary of the capabilities of social media, but I have a much deeper understanding of the multiple strategies that allow it to be used in information warfare.

As a takeaway, I now understand social media as a tool that can cause change and will be more cautious with how different platforms will affect my behavior. Yet, I am more interested in learning about social media algorithms and trying to understand their insides better to inform myself and others about possible implications.

CONCLUSION

These topics have been fascinating to learn about and have effectively deepened my understanding of cybersecurity ethics. Corporate Social Responsibility is effective in learning about the connection between business and their consumers and that it's a primary objective for the relationship to be functional and beneficial. Whistleblowing, as an action, is a complex choice that, while it may be the result of there being no other options for information to be known to the public, it is an act that can show dedication to an organization's values or a desire

to protect the public that is being harmed in some way, shape, or form. Due to Information Warfare relying on cyberspace, avenues like social media and other platforms have the potential to be used as weapons that can easily spread misinformation to cause chaos, hence why it is critical for there to be a greater understanding of algorithmic capabilities to protect the information of many people. To sum up, this class has been instrumental in helping me to consider multiple perspectives on topics within the cybersecurity industry, and I plan to remember it as a valuable tool in the future.

WordPress Website Link: https://sites.wp.odu.edu/epres010/law-ethics/phil-355e/