Noah Huber

Professor Henderson

CSCI 325

23 March 2024

The Ethical Implications of Cybersecurity

Cybersecurity is a continuously growing field following the constant expanse of digital technologies. The importance of safety and security online is becoming more imperative as the availability and attainability of technology has significantly increased over the last decade. There is a prominent growing need for cybersecurity professionals to ensure that systems and data are protected and secure. This helps systems run efficiently and ensures that they are safe from threat actors. Pursuing a career in cybersecurity gives me the balance between physical hands on and software. Cybersecurity also gives opportunities to delve into criminal justice and pursue threat actors for their harmful actions, thus contributing to a safer digital landscape for individuals and organizations. The workload from this career can spread from cyber analysts to a Certified Information Systems Security Officer (CISSO). Traversing over a range of daily tasks that will have both digital and physical interactions with people.

Cybersecurity professionals are involved with many different systems and utilized by many different organizations. Modern implications of cybersecurity professionals help keep systems protected and secure, monitoring traffic and data that goes in and out. Cybersecurity professionals can be implemented in many different situations and work for many different organizations. This widespread opportunity of work can lead to cybersecurity workers being exposed to data and even sensitive data that brings up concerns of privacy and ethical challenges. According to Rod Trent, in an article about the ethics of cybersecurity, “However, cybersecurity

also poses ethical challenges and dilemmas, such as the trade-off between security and privacy, the responsibility and accountability of cybersecurity professionals, and the regulation and oversight of cybersecurity practices." (Trent, 2024) There are plenty of examples of ethical dilemmas posed to cybersecurity professionals that may be faced daily. One of the biggest ethical dilemmas that I may face when venturing into the field of cybersecurity, is the protection of healthcare systems.

One of the leading organizations that utilize cybersecurity professionals is healthcare, including hospitals and doctors' offices. Many of these organizations have databases and servers that contain sensitive information about patients, doctors, and more. Cybersecurity professionals, including CISSO's, are essentially exposed to thousands of pieces of sensitive data, including social security numbers, dates of birth, addresses, and financial information. The exposure to such sensitive data and constant decision-making can bring up ethical challenges and dilemmas for cybersecurity professionals. These ethical issues include balancing privacy over security, determining appropriate access control measures, and considering the ethical implications of whistleblowing in cases of unethical or illegal practices that jeopardize patient data security. Cybersecurity professionals in healthcare must navigate these ethical dilemmas while upholding principles of integrity and protecting the confidentiality and privacy of patients' sensitive information.

To effectively handle and overcome ethical dilemmas in cybersecurity, it's crucial to start by understanding what a strong ethical foundation is. A strong ethical foundation includes an understanding and adherence to industry standards, regulations, and ethical guidelines.There are many ethical guidelines like the ACM Code of Ethics and Professional Conduct and the IEEE Code of Ethics. Additionally, staying informed about emerging technologies and evolving threats

is essential to anticipate potential dilemmas proactively. Personally, I believe in continuous learning and development, both in technical skills and ethical decision-making. It is also important to me as a man of God to seek out his wisdom and guidance whenever I am faced with a challenge or any ethical dilemma. As a confident leader, I will actively seek out opportunities for training, workshops, and certifications related to cybersecurity ethics and best practices. Increased consistent training can help defend against many cyber threats. Ultimately strong communication and critical thinking skills are essential for navigating complex ethical situations.

As a sophomore, it is somewhat far out to plan on specific actions that I would take in my career. However, I plan to regularly assess and update my knowledge of relevant laws, regulations, and industry standards to ensure compliance and ethical conduct in my work. I plan on ensuring my understanding of my career field and the ever-evolving world of digital technology. Additionally, I will prioritize networking, and creating relationships with peers and mentors whom I can consult with and seek guidance from when facing challenging ethical issues. I plan to develop a foundational decision-making framework that considers ethical implications alongside technical requirements. This will not only demonstrate my leadership skills to take action when needed but also keep me well-versed in my career. The key to overcoming ethical dilemmas is staying vigilant, proactive, and committed to proper ethical conduct. If any questions arise that cannot be answered by a person can be answered by God.

The ACM Code of Ethics and Professional Conduct sets the foundations demonstrating the importance of contributing to society and human well-being through computing, acknowledging the interconnectedness of all people in the digital age. The first principle which I find one of the most important is, “This principle, which concerns the quality of life of all people, affirms an obligation of computing professionals, both individually and collectively, to

use their skills for the benefit of society, its members, and the environment surrounding them." (ACM, 6) A higher quality of life will highlight respect and a quality of life that supports human well-being. This principle is prominent in Biblical teachings that emphasize the command to love one's neighbor and serve others. In Romans 12:10, Paul instructs the church to "Love one another with brotherly affection. Outdo one another in showing honor." (Romans 12:10, ESV), embodying a spirit of compassion and service. This action of outdoing one another in honor displays dignity and respect towards others, following the ideologies of the first principle. Additionally, Proverbs 14:31 highlights the significance of kindness to the needy as a reflection of honoring God, "Whoever oppresses a poor man insults his Maker, but he who is generous to the needy honors him." (Proverbs 14:31, ESV) Thus, by aligning with the ACM principle, individuals in the computing field uphold Biblical values of compassion, service, and social responsibility, recognizing the inherent dignity and worth of every individual.

Similarly, the IEEE Code of Ethics prompts the upholding of integrity and fairness by advocating for the avoidance of real or perceived conflicts of interest. The IEEE Code of Ethics instructs, "to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;" (IEEE, Section 7.8) Colossians 3:9-10 urges followers of Christ to embrace honesty and transparency, reflecting the character of God in their conduct. "Do not lie to one another, seeing that you have put off the old self with its practices" (Colossians 3:9, ESV) Adhering to the ACM and IEEE principles, professionals in technology and cybersecurity demonstrate proper ethics that reflect the integrity and truthfulness also encouraged by Biblical teachings. ACM and IEEE codes not only provide ethical guidelines for professional conduct but also align with Biblical teachings that guide individuals in their interactions with society and interpersonal communications.

Works Cited:

Association of Computing Machinery. *ACM Code of Ethics and Professional Conduct Booklet*. 2018, https://doi.org/10.1145/3274591. Accessed 19 Mar. 2024.

IEEE. "IEEE Code of Ethics." *Ieee.org*, June 2020, www.ieee.org/about/corporate/governance/p7-8.html. Accessed 19 Mar. 2024.

Study Bible-ESV. English Standard Version, Crossway Bibles, 2014.

Trent, Rod. "The Ethics of Cybersecurity." *Rod's Blog*, 17 Jan. 2024, rodtrent.substack.com/p/the-ethics-of-cybersecurity. Accessed 19 Mar. 2024.