Jessica Taylor

Professor Henderson

CSCI 235-01

April 1, 2023

An Ethical Dilemma in Cybersecurity

Modern day society in developed countries depend on the use of technology. As technology evolves and becomes more capable, individuals and organizations use technology to store important, personal, and/or confidential information. Thus, cybersecurity professionals are challenged now more than ever in the use of critical and abstract thinking to secure important information. Often, cybersecurity experts find themselves gaining access to sensitive information which they may not agree with or find interesting and have a strong urgency to share the information. This is where the ACM and IEEE code of ethics play an important role in maintaining balance between discovering/securing sensitive information and what to do when information is discovered which may be harmful to an individual or society. As a cybersecurity professional, it is important that one must know and follow the legal, ethical, and moral stipulations of securing sensitive information.

To start, the ACM and IEEE are both entities which maintain separate outlines of professional code of ethics within the computer science and engineering communities. The general principles of the ACM code of ethics include responsibility to “contribute to society, avoid harm, honesty and trustworthiness, avoid discrimination, respect creativity and privacy, and honor confidentiality” (ACM 2023). Similarly, the general principles of the IEEE code of ethics include responsibility to “uphold the highest standards of integrity, responsible behavior,

and ethical conduct in professional activities; treat all persons fairly and with respect; strive to ensure this code is upheld by colleagues and coworkers" (IEEE 2023). There are a couple differences between the ACM and IEEE code of ethics. One difference is the ACM code of ethics not only includes the general principles of the code, but also includes professional responsibilities, leadership principles, and code compliance. Secondly, the ACM code appears to apply to computing professionals, whereas the IEEE code applies to a broader group of individuals within the engineering and technology professions.

In addition, Christian cybersecurity professionals should consider how teachings in the Bible align with the ACM and IEEE ethical codes. While all principles outlined in both ethical codes are important and relevant to cybersecurity professionals, there are certain principles that specifically pertain to confidentiality and avoiding harm. The ACM code of ethics states "…respect privacy and honor confidentiality…" (2023), while the IEEE code of ethics says, "To treat all persons fairly and with respect, to not engage in harassment or discrimination, and to avoid injuring others" (2023). Additionally, the Bible contains many passages which align with the ethical principles outlined in the ACM and IEEE, one in which 1 Corinthians 10: 23-24 (NIV) states, "'Everything is permissible" – but not everything is beneficial. "Everything is permissible" – but not everything is constructive. Nobody should seek his own good, but the good of others" (Bible Gateway n.d.). Individuals working in cybersecurity roles should remember the code of ethics outlined in the ACM and IEEE along with God's teachings outlined throughout the Bible, all of which should be referenced when making decisions regarding one's sensitive or personal information.

To continue, a realistic scenario which a cybersecurity professional (including myself) may experience is one in which sensitive/personal information is discovered which may indicate a possible threat to one or more members of society. This proves to be an ethical dilemma because a cybersecurity professional is to maintain confidentiality of information found during the process of maintaining security. While this is a difficult situation with many right and wrong paths a cybersecurity professional may choose, it is likely best to first continue to maintain confidentiality and ask the client about the potentially harmful information. If it is not within the professional's scope to have direct contact with the client, then the next best option is for the professional to notify their upper management of the potential threat. Either way, if a potential threat is identified, further steps should be taken to mitigate the threat. These actions should always follow legal and ethical guidelines.

Finally, an upcoming cybersecurity professional, such as I need to be prepared for ethical dilemmas, which we will face at some point in our career. The first step in preparing for managing situations in which ethical dilemmas arise is knowing and understanding the ACM and IEEE ethical codes. These codes will serve as basic moral and ethical guidelines for managing difficult situations. In the case of the previous example in which a cybersecurity professional finds information which may be a threat to one or more individuals, it is important for a professional to know one's bounds. For example, the way I would personally prepare for this situation is to first, ask my upper management who I should or should not notify shall I find myself in this situation. Typically, there are guidelines for such situations which involve ethical dilemmas, and it is important to be familiar with the guidelines to ensure the safety and protection of oneself and others.

In conclusion, as a cybersecurity professional, it is important that one must know and follow the legal, ethical, and moral stipulations of securing sensitive information. Why is it important that cybersecurity professionals have a code of ethics? The answer to this question is evident in the ever-evolving capabilities of technology and the professionals responsible for securing such technology. An example of technological advancement is artificial intelligence. Computing professionals have the capability to create real harm to society in how AI is programmed/used. Cybersecurity professionals have the knowledge and skill to gain unauthorized access to AI technology and alter the way in which it functions with the intent to cause harm. Part of the ACM/IEEE code of ethics (in addition to the ethical teachings of the Bible) include the responsibility to do no harm. AI is a real world, legitimate example of why it is important for both computing and cybersecurity professionals to not only have but follow a code of ethics.

Works Cited

"Bible Gateway Passage: 1 Corinthians 10:23 - New International Version." *Bible Gateway*, https://www.biblegateway.com/passage/?search=1+Corinthians+10%3A23&version=NIV.

"The Code Affirms an Obligation of Computing Professionals to Use Their Skills for the Benefit of Society." *Code of Ethics*, https://www.acm.org/code-of-ethics.

"IEEE Code of Ethics." *IEEE*, https://www.ieee.org/about/corporate/governance/p7-8.html.