Justin Pike

Professor Julie Henderson

CSCI 325

11 June 2022

Ethical Dilemmas in Cybersecurity

The Internet offers the world the single greatest apparatus for information exchange and access to the breadth of human knowledge and history that the world has ever seen. Every day there is a quantifiable yet still unimaginable amount of data traverses that globe in an instant in this electronic environment. This data is comprised of private information and transactions of the average citizen of the world to the business data that drives the world around these citizens and then even classified data requiring the utmost security. The astronomical growth of the Internet since the early 2000's, and its continued proliferation now and into the future has created a great demand for cybersecurity professionals to aid in the constant struggle to protect the integrity of data for citizens, corporations and even intelligence agencies. However, entrusting not only advertent but also inadvertent access to personal, public, and private sector data to cybersecurity professionals poses its own set of risks and can place individuals these individuals in precarious ethical dilemmas. The concept of confidentiality is of paramount concern for cybersecurity analysts/technicians behind only the security of data itself and is the most frequent problem that will be encountered by computing professionals that protect or monitor the data of others.

The concept of the release or misuse of private and proprietary information/data by the very individuals that are intended to protect is far from new and insider threats are one that most companies and government organizations know all to well from experience. The perpetrators of such actions are comprised of whistleblowers, those seeking financial gain or publicity and even those pressured by foreign governments. According to the Computing Technology Industry Association, those individuals working in a cybersecurity capacity, “see and handle personal, private or proprietary information that should be kept strictly confidential” (“Ethical Issues in Cybersecurity”). Confidentiality as defined by Oxford, is “the process of and obligation to keep a transaction, documents, etc., private or secret” (“Confidentiality”). Interestingly, cybersecurity is one of very few job fields where a breach of confidentiality would go directly against the actual purpose of the cybersecurity role. By their very nature and with access to the electronic secrets of the world and individuals, cybersecurity and computing professionals are placed in a position of trust and confidence with a constant pressure to not misuse and abuse their position. This pressure to utilize their position, with access to private information, can take the form of an internal struggle for personal gain or outside pressure of other individuals such as news/media organizations, competing companies and even foreign entities. Breaches of trust with the handling of information can have far reaching implications and can cause tremendous unforeseen harm. One well-known instance of is that of Edward Snowden, in which, he as Information Technology contractor for the National Security Agency knowingly downloaded millions of classified documents and released a substantial number of them to the media, causing tremendous harm to national security and negatively affecting the United States in the political, economic, and social spheres (Arslan and Quarcoo).

The pressures of maintaining confidentiality as part of the cybersecurity role is a consideration that no individual should take lightly when contemplating the field as a potential employment opportunity. Much like the jobs of an intelligence analyst or that of a lawyer, there is expectation that information will be presented to a cybersecurity professional that may conflict with the personal value system of that individual, but that they will still be required to keep quiet about that information and keep it confidential. This is not to say that there might not be information that may be a blatant violation of the law, but there are systems and procedures in place to handle these instances. These protocols are actually put in place by organizations and agencies in order to alleviate the personal dilemma and take the ownership of the problem off of the individual. Personally, I know that I am and will be prepared for any information that I may encounter and have to keep confidential, because I have worked in the intelligence community for over 12 years and have had to learn to be okay with this type of knowledge in my mind. For those who lack experience in dealing with information handling, perhaps the negative consequences to their current and personal careers will be enough to dissuade them from breaching confidentiality. A breach of this type directly reflects on the character and value system of the individual and will most likely dissuade any potential future employer from hiring them, especially in the information technology fields. For those individuals who still may require more guidance in the realm of confidentiality, the Bible, as always, offers a unique and concrete perspective on God directs everyone to live.

Ethical behavior in the fields of computers and technology are well defined in the Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct and the Institute of Electrical and Electronics Engineers (IEEE) Code of Ethics. The ACM Code of Ethics focuses on the ethical behavior of the computer specialist as an individual and the responsibilities that they have not only to their employers but also to others within their community. As defined by Section 1.7 Honor confidentiality, “Computing professionals should protect confidentiality except in cases where it is evidence of the violation of law, of organizational regulations, or of the Code” (“ACM Code of Ethics and Professional Conduct”).

This section specifies that there are instances where disclosure may be needed, but that the disclosure needs to be handled appropriately and through the correct channels. The Bible addresses the concept of confidentiality by not only making clear that keeping confidence is a reflection of the trustworthiness of a person, but also directing individuals to "guard what has been entrusted to you" (*New Living Translation*, Prov. 11.13, 1 Tim 6.20). As a governing body for a number of the technologies that drive the electronic world, the IEEE has a similar code of ethics but is more focused ensuring the ethics behind the technology and the organization that that of the individual user. Bribery is an issue which is taken very seriously within the IEEE as there cannot even appear to be any measure of favoritism or towards specific companies, vendors, developers or even counties when the technology will inevitably affect every person in the world in some fashion. IEEE Code of Ethics Section I.4 states that member agree "to avoid unlawful conduct in professional activities, and to reject bribery in all its forms" ("IEEE Code of Ethics"). The Bible clearly directs that God's people "shall not take a bribe, for a bribe blinds the clear-sighted and subverts the cause of the just" and that those who decline a bribe prosper (Exo. 23.8, Prov. 17.8)

Confidentiality is a concept that is expected in a number of areas of life and is increasingly becoming a key qualification for jobs as more of everyday life becomes electronic. The field of cybersecurity is charged with the protection and security of the data and thereby the secrets of the world and cybersecurity professionals are constantly faced with the potential confidentiality issues as they monitor data. By adhering to current and future ethical standards set for by computer and technology organizations, company policies and looking to the Bible for guidance to right living and good/moral behavior, the specialists can effectively execute their duties, demonstrate their character, trustworthiness and be a model of good/moral behavior for others to emulate.

Works Cited

"ACM Code of Ethics and Professional Conduct." *Code of Ethics*, https://www.acm.org/code-of-ethics#h-1.-general-ethical-principles.

Arslan, Hasan T, and Joyren Quarcoo. "Political, Economical and Social Impacts of Snowden Breach." *Pakistan Journal of Criminology*, vol. 7, no. 2, Apr. 2015, pp. 29–42.

"Confidentiality." *Oxford Reference,* https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095631575.

"Ethical Issues in Cybersecurity." *CompTIA's Future of Tech*, https://www.futureoftech.org/cybersecurity/4-ethical-issues-in-cybersecurity/.

Holy Bible. New Living Translation, Tyndale House Foundation, 2013.

IEEE Code of Ethics. https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/corporate/ieee-code-of-ethics.pdf.