Jacob Braddock

Professor Julie Henderson

CSCI 325

23 Mar. 2024

Growing Concern of Ethics

It has been spoken before and been a heavily talked about topic of the growing ethical concerns of the computer work industry. This goes for programming, software development, cybersecurity, or anything between such fields of work. Fact is, as the modern age chugs on and the progression of modern developments occurs and evolves, we are left with a growing concern in the violations of ethics and how we should handle such a thing. These dilemmas that we confront need to be studied and figured out as the future approaches, how to handle such dilemmas, and a bit of a biblical view on some of the most respected computing moral code that exists.

Given my major with cybersecurity and likelihood of me heading into that field, there are daily moments of me considering the ethics of what I am doing. One of those dilemmas would be the detection of vulnerabilities within a system. There are many ways to go about this, though how you handle such things can quickly violate any morality in such a thing rather quickly. While one may find something wrong with the security of a company website or system, there could be quick legal repercussions for such a thing. Mirko Zorz in an interview with Eddie Zhang, principal consultant of Project Black, states that “A company will aim to avoid negative publicity. Opting for full public disclosure can apply pressure to the affected organization to fix the issue, however this pressure can also manifest itself into a legal pursuit against you (Zorz)”. This means the need to jump through, many hoops to disclose such a vulnerability, and taking the proper legal route to do such a thing. These disclosures, however, need to come out at a speedy timeframe, especially with recent passages of laws and orders by the government itself. As recent as 2021, "The United States Securities and Exchange Commission (SEC or Commission) recently issued two critical Consent Orders, First American Title and Pearson, both articulating the need for timely, fulsome, and accurate disclosures to the market when a data breach occurs (Ferrillo et. Al.). This means there needs to be a proper balance in notifications of breaches and vulnerabilities, while also trying to avoid legal hurricanes in the wake of what you may say. Like a walk across a balance beam, a look down before a high dive, the balance of ramifications and doing the morally correct thing need to all be done properly and preparing the outside world for what has happened or what could happen. This includes within the company itself as well, as humans are always the biggest concern when it comes to that of the passage of information that should not get out. Through primarily file sharing or vocal contact, there should be a minimization of employee sharing of such info with it instead reaching the higher ups first. This goes beyond malware type files as well, as "Data sensitivity and privacy are also relevant here, considering the growing number of data regulatory policies such as the General Data Protection Regulation the California Consumer Privacy Act and countless other data protection laws (Groopman)" have cropped up in large amounts with the expansion of online traffic. This means that creating vulnerabilities and compromising situations is prevalent and a major risk to ethical violations.

I think when it comes to these violations, people need to do mainly two things. Talk with higher ups and what they expect and follow their common sense. In this field there is no real room for error in this field, and with most employees of the cybersecurity field needing to be always on their toes, there needs to be a sense of constant thought process of what should be done. This is what concerns me the most when I enter the work field. I want to do the right thing the right way, and the problem is I may just not do it like I should. Anyone can have good intentions when it comes to doing xyz number of things, but they can easily mess up and have those intentions dashed in an instant into a major mistake. I want to follow my senses and a good moral code to make sure I don't break ethical expectations.

In terms of a good moral code, there are two major ones I have written about before in other ethics papers being the ACM and IEEE code of ethics. To start with the ACM, I think that section 1.2 in avoiding harm is the most important to me, especially if I looked at it from a biblical type of worldview. The Bible often talks of being a morally correct person, and this is seen in talks of avoiding harm to those around you. In Philippians 2:4 it says to "not look to your own interests, but each of you to the interests of others (NIV, Philippians 2:4) which I find to be extremely in line with that of the Code of Ethics section for the ACM and just for cybersecurity in general. We are the people who need to protect others, and this means valuing the safety of others, doing what we can to help them out. As for the IEEE code of ethics, in section 2 or II as it is listed, it talks about treating those fairly. I find this to be extremely important within the field of cybersecurity and life in general for that regard as no one should be treated differently in upholding the ethics that comes with cybersecurity. In the bibles, it states that "God does not show favoritism (NIV, Romans 2:11). If the Lord himself does not treat anyone differently to the next, then why should I do it differently? I must uphold morality and protect everyone around me, no matter who they may be.

I am scared to continue into the big world. I wish and desire nothing more to do my job to the best of my abilities while also protecting those around me as best as I can. If disclosing vunerabilties and data breaches is what I must do to uphold that desire, then I shall do such a thing while staying in the line of what is morally acceptable and just. In my own views, the views of the bible, the views of ethics, and views of what is right in my workplace, I will uphold the safety and sanctity that exists. There needs to be protection for all, and we as the protection workforce must do it the right way.

Works Cited

Bible.Com. NIV, 2011, https://www.bible.com/bible/111/php.2.4, Accessed 23 Mar. 2024.

Biblegateway.Com. NIV, 2011, https://www.biblegateway.com/passage/?search=Romans%202:11&version=NIV, Accessed 23 Mar. 2024.

Groopman, Jessica. "7 Common File Sharing Security Risks: TechTarget." *Content Management*, TechTarget, 21 Sept. 2022, www.techtarget.com/searchcontentmanagement/tip/7-common-file-sharing-security-risks.

Zorz, Mirko. "Vulnerability Disclosure: Legal Risks and Ethical Considerations for Researchers." *Help Net Security*, 21 Nov. 2023, www.helpnetsecurity.com/2023/11/27/eddie-zhang-project-black-vulnerability-disclosure/.

Zukis, Bob, et al. "Cybersecurity and Disclosures." *The Harvard Law School Forum on Corporate Governance*, 4 Oct. 2021, corpgov.law.harvard.edu/2021/10/04/cybersecurity-and-disclosures/.