Bryce Furrow

CSCI 325

Professor Julie Henderson

26 March 2021

Ethics of Vulnerability Disclosure

There are many ethical concerns in the workplace, but one area that seems to be expanding immensely as technology improves over time is the massive and diverse field of programming. In a world that is becoming increasingly more interconnected, those in the fields of programming are having more and more put on their shoulders, including being faced with entirely new situations with moral and ethical concerns in question. Those leading in the technological fields recognized this and created their own codes of ethics to flesh out many of the guidelines for their peers of the present and future to utilize and consider for themselves. I will reflect on two of them, the ACM and IEEE Codes, with my own personal thoughts and Christian beliefs in regards to a major ethical concern in my future career.

The field that I will be heading towards working in is that of programming and cybersecurity. They have, and share, a wide number of ethical dilemmas, but the primary ethical concern that I may personally face in my field of work – especially in cybersecurity - is that of vulnerability response and disclosure. Vulnerability disclosure is the degree of "openness and transparency among security researchers, security vendors, and other stakeholders" (McKinney 1). It is about the communication of breaches, flaws, and other discrepancies of a product, service, system, etc., "balanc[ing] equities and mak[ing] determinations regarding disclosure or restriction" between the primary customers and the general public (Huskaj 105). Even with this

single topic, there are multiple aspects that should be addressed when analyzing it ethically. There is the question of when customers should be informed of a breach, and, additionally, how should they be informed. There is also the concern of how much detail should they be given when they are debriefed of the situation. Now reflect these same questions with the general public in mind. When and how should they be notified, and to what degree of detail? This issue has many divided – far beyond just the world of cybersecurity as well. Some people believe that total transparency and detailing should be done as soon as the event is identified and assessed, arguing that it "increases public awareness, pressures vendors to issue high-quality patches quickly, and improves software quality over time" (Arora and Telang 1). Critics of this method state that this is irresponsible and dangerous, especially without first finding the best way to solve the breaches (Arora and Telang 1). This would be because it opens the floodgates for public distress without any solution to fix it, and it shows the attackers that you discovered them – allowing them a way out or do further damage before properly countering. These are all just some of the considerations on a single topic within the ethics of working in the fields of programming and cybersecurity. It is something that I will definitely have to face at some point in my career if I move further into the field of cybersecurity.

In terms of handling this issue, there are ways that one would - and should - be able to prepare for it in advance. Generally speaking, since this issue is somewhat straightforward, so too are the ways to prepare for it. One thing that one should do to prepare for handling this ethical issue is to become more educated – not just in both the fields of programming and cybersecurity, but also to learn more in regards to business economics, sociology, and public relations. Looking more into these topics will allow one to make a more measured decision that is best for this situation. Another thing that one should do to prepare is to seek to build one's own

character in order to formulate a strong moral and ethical compass. This would be less specific to the issue, but it will be applicable to all ethical obstacles that one will face – in the workplace and outside of that. The catalyst for this moral focus should, undoubtably, be found in God's Word and following Him in one's life (2 Timothy 3:16, NIV, 2011). As for myself, I will seek to be practicing what I preach (1 John 3:18, NIV, 2011). In order to prepare for this ethical dilemma (and for others of similar caliber), I plan to specifically take classes here at Charleston Southern University regarding business, economics, philosophy, and Christian studies. Additionally, I will look into these same topics online along with that of Biblical philosophy and public reactions to events similar to ones that I may be a part of in the future. I will also seek to build up communication and relational skills since it will better my future, even if I do not end up in the field where I am headed now. It would allow for me to better manage these ethical situations and find solutions to the problem in coordination with others involved. Something that would support me as I move forward in all of the previously stated ways is finding professional and spiritual mentors around me so that I may be aided in building myself up and pushing forward (Proverbs 15:22; 19:20-21, NIV, 2011). As for how I feel about my ability, right now, to face these challenges, I know that I have a long way to go. However, I feel that there is no better place than Charleston Southern University to cultivate my character by promoting academic excellence in a Christian environment.

In regards to professional codes of ethics outside of my own, there are two primary ones that I will cover – the ACM Code of Ethics and Professional Conduct and the IEEE Code of Ethics. Overall, the ACM Code of Ethics principles are focused on those in the computer science field, containing both general and specific guidelines. These can be summarized as follows: be beneficial and morally good for the sake of society and humanity, with everyone held in mind as

stakeholders to your work; as a professional, you should do your best in all that you do, keeping in mind the moral commitments and stakes at hand; leaders should be virtuous, responsible, and aware of group opportunities and the status of the individual members within the group; and the code should be maintained faithfully ("ACM Code of Ethics and Professional Conduct"). The IEEE is aimed to a more general target group of those involved in professional technological fields, including, for example, engineers and other such fields ("IEEE Code of Ethics"). The IEEE's principles can be summarized as follows: maintain professionality in all working circumstances with ethical and practical concerns in mind, including the integrity and objective standards of legality and working against obstacles like conflicts of interest; treat everyone respectfully in all aspects, regardless of who they are and what they personally believe, which also extends to their property, reputation, etc.; and maintaining the constant use and consistent application of this code in the workplace, holding due punishment for those who violate it ("IEEE Code of Ethics"). In terms of similarities between these two codes, there are many that can be listed. Both of them include these things: public good and the consideration of one's own actions and work with that in mind, protection of privacy and confidentiality, maintaining to the legal system in place, holding morally good values like respect, responsibility, integrity, and fair treatment of others, and that their respective code should be maintained faithfully ("ACM Code of Ethics and Professional Conduct"; "IEEE Code of Ethics"). They didn't have as many differences as I had expected previous to reading them for myself. The ACM Code goes into excruciating detail with categories, points, and subpoints within those, but the IEEE Code speaks far more generally on its categories and its points ("ACM Code of Ethics and Professional Conduct"; "IEEE Code of Ethics"). The ACM Code focuses more heavily on programming and ethics regarding that, and the IEEE Code focuses a bit more on the aspects of professionality

("ACM Code of Ethics and Professional Conduct"; "IEEE Code of Ethics"). Many of the social and work ethic concerns in both of these codes follow very similar ideas to that seen in the Bible. One example of this from each code is the ACM's statement of being honest and able to be trusted and the IEEE's statement to listen to and accept criticism ("ACM Code of Ethics and Professional Conduct"; "IEEE Code of Ethics"). Reflecting what was seen in the ACM, the Bible states, "The LORD detests lying lips, but he delights in people who are trustworthy" (Proverbs 12:22, NIV, 2011). Reflecting what was seen in the IEEE, the Bible states that people should "be quick to listen, slow to speak and slow to become angry, because human anger does not produce the righteousness that God desires" (James 1:19-20, NIV, 2011). While it is obvious that the reasoning for the two Codes of Conduct is different from that of the Bible, they are most definitely supported by those Biblical views.

Now we may return to the original concern of the major ethical dilemma that I am likely to face in my career's future – vulnerability disclosure. Despite both the ACM and IEEE Codes regarding the importance of the public good in one's foremost considerations of one's own works, after reviewing both of these codes of conduct, it is made very clear that the ACM Code is far more relevant to my current field of programming and cybersecurity; therefore, the ACM Code will be more apt for me to apply. To start off, it is clear that lying about the vulnerability disclosure is not viable to the ACM Code, nor is it a major stance that is taken by those that hold discussions about it, as we had covered earlier ("ACM Code of Ethics and Professional Conduct"). In terms of the main stances, it can be determined that the code opposes the extremes - little to no disclosure and total disclosure. This is because, little to no disclosure clearly contradicts the rules verbatim stating the need for public disclosure ethically, and the total disclosure – in the fullest sense discussed early on - violates the rules of confidentiality, privacy,

and the security of the company and possibly its customers as well ("ACM Code of Ethics and Professional Conduct"). In addition, there is a rule to "avoid harm" that refers to "negative consequences, especially when those consequences are significant and unjust," and one of the examples given for this is "unjustified destruction or disclosure of information" ("ACM Code of Ethics and Professional Conduct"). With this in mind, while it doesn't give a direct answer to the question, the prelude to the code itself states that it was never written with the intention of being followed like an "algorithm" ("ACM Code of Ethics and Professional Conduct"). It can just be stated that the disclosure of vulnerability should be present and performed properly for all breaches that put the company, the customers, and/or the public at risk, but not being so total as to violate those that they wish to aid, and, at the same time, not so negligent as to leave them unjustly unaware of the threats being faced. As it was stated earlier, both extremes have their negative sides that end up working against the public good cited as a crucial focus for the ACM Code ("ACM Code of Ethics and Professional Conduct"). As a final statement, I personally agree with the idea of staying off of the extreme ends of the conflict, and I believe that each situation is also unique and should be judged accordingly with the good of the company, the customers, the public good, and my own personal Christian ethic in mind.

Works Cited:

"ACM Code of Ethics and Professional Conduct." *Acm.org*, 2018, https://www.acm.org/code-of-ethics. Accessed 26 March 2021.

Arora, Ashish, and Rahul Telang. "Economics of software vulnerability disclosure." *IEEE security & privacy* 3.1 (2005): 20-25.

Huskaj, G., and R. L. Wilson. "Offensive Cyberspace Operations and Zero-days: Anticipatory Ethics and Policy Implications for Vulnerability Disclosure." *Journal of Information Warfare* 2021.20.1 (2021): 96-109.

"IEEE Code of Ethics." *IEEE.org*, https://www.ieee.org/about/corporate/governance/p7-8.html. Accessed 26 March 2021.

McKinney, David. "New hurdles for vulnerability disclosure." *IEEE Security & Privacy* 6.2 (2008): 76-78.

New International Version Bible (2011). Zondervan.