Tyler O’Hare
CPRE 234

# Cyber security Code of Ethics

In this paper, I will discuss my personal code of ethics for the cybersecurity industry. First, I will discuss some of my personal ethics and how my understanding of them has changed throughout my time taking this class. Then I will go over some of the skills that I think will be important for my code of ethics as well as which of these skills I feel I struggle with. In class, we defined a code of ethics as, “An attempt to reconcile individual or cultural differences into a unified set of guiding principles or duties.” Before taking this class I didn’t really know what a code of ethics was specifically. But after covering some examples, I can see why they are important from both a psychological perspective and a perspective of wanting to implement a strong “foundation” of rules. As we discussed in class, my code of ethics is not all-encompassing and similar to other codes of ethics, should be considered a minimum in pointing in the direction of what I believe is the ethical way to behave.

The first part of my code of ethics I want to discuss is about being an ethical individual both inside and outside the work environment. To me, it is important to not have to live too much of a double life when it comes to personal and work life. This plays into some of the soft skills I will discuss later on in this paper regarding trustworthiness, dependability, and the ability to act as a “leader”. Along with this, I would not want my personal code of ethics to conflict with the code of ethics that resides in the organizations I am working with. This could lead to an ineffective work environment and make mutual benefit difficult. If an organization wants me to perform an act that I deem goes against my personal code of ethics, I will do whatever is possible to withdraw from that organization.  One of the codes of ethics we covered that I thought was interesting was the ISC2 code of ethics. I feel like the ISC2 code of ethics resonates strongly with this first part of my code of ethics because it focuses on acting in the welfare of society as a whole in contrast to doing what is only good for you or the organization that you are working with. The next part of my code of ethics gives an example of this.

At the beginning of the semester, I did not have a very clear understanding of code of ethics when it came to cybersecurity. Although I thought I would’ve been prepared for most situations that would come up in the field and life, I was then introduced to something called ethical dilemmas. As we talked about ethical dilemmas in class I became more aware of how unprepared I would be to make decisions regarding these tough situations. From this, I learned the importance of developing or utilizing some sort of external sources or frameworks that lays down some set of hard rules to deal with these situations. You may sometimes be put in a situation where what your organization wants you to do is not in the best interest of many others in the society around you. In most cases in cyber security you will not need to make a decision that will result in damages on both sides of the decision. That being said, you never really know when something bad will happen to the organization that you work with and it is never a good idea and wait for something to happen of consequences for you, your organization, and society as a whole. Therefore, I think it is important to put in my code of ethics to never struggle alone. When I am in a situation I don't feel like I can handle alone I should always seek some form of guidance. Then based on the results of that, make an educated decision. Tools like The Ethical OS toolkit are a perfect example for reflecting and preparing solutions to difficult situations when they happen. Because of this, I think it is in my best interest to consult multiple opinions/ frameworks before dealing with things like ethical dilemmas in an organization or for myself. Receiving help from outside sources when you are unsure can be crucial to expanding your scope of understanding and making the right decision when the answers are not so clear-cut.

In our lecture, we talked about how in cyber security there isn't really any "absolute security", in other words, you can't really reach perfection in security and there will probably always be at least one threat you are not safe from. I feel like this is an idea that should be taken into my code of ethics because it helps take off a lot of the stress of trying to be perfect in the field. You do not need to have the best solution in every situation, but simply have a correct solution that helps to mitigate issues with the resources that you are provided. Another thing that I want to add on to that with, "security often comes with a trade-off". Security is not always going to be the best solution whether it is in personal or even corporate life. Most of the world is too lazy to use things like VPNs and tracker blockers every time they want to visit a website. But if people wanted to have the best security they would be using these things wouldn't they? The trade-offs that come with using things like these can vary from person to person but usually fall into a few categories. One category I think everyone is concerned with is speed. In some cases, using things like VPN or highly effective encryption/decryption algorithms can really slow down the speed of one's network or computer. Most people just would not want to make the trade-off of their speed and productivity in order to have the best security standards. Similarly in the corporate world, companies may not have security at the forefront of their priorities. They usually want to focus on productivity and making profits. Keeping this in mind is crucial in my opinion because it means you are going to need to find ways to bring the importance of security to the forefront for the organizations you work for. I will talk more about this when I cover which soft skills I think are important for implementing my code of ethics and the importance of being a persuasive and good technical communicator.

Soft skills are one of the most important things to have for just about any technology or engineering field. For cyber security there are three soft skills in particular I think are the most important in developing. The first of the soft skills I think is important is being able to maintain trustworthiness and credibility with those you work with. The second being able to communicate important technical concepts to those who don't have experience in the field. And the third being able to work effectively with others under pressure.

The foundations of cyber security are based on the idea of trustworthiness and authenticity. These fall under the scope of integrity in the C.I.A triangle. In my opinion, this triangle doesn't just apply to the technology that cyber security professionals use, but also the professionals themselves. The reason this soft skill is important to me is that without being able to be trusted by people you are working with, how do you expect to get anything done? If you have a history of being untrustworthy and undependable nobody will want to give you the keys to their organization’s security.  Additionally, in cyber security it is not a good idea to try to play the “fake it till you make it” attitude. In my opinion, it is much better to be able to “walk the talk” and be honest when you are not sure about something. This brings you off as a more honest person and people will trust you more for that.

Being able to communicate technical information is a very important soft skill for those in a cyber security profession due to the fact that if people don’t understand the information you are trying to communicate and its importance, you may fail to deliver fully on your job. You may find something that is considered a huge threat to your organization’s security and it needs to have a major rehaul done to the system in order to remove the possibilities of this threat. This rehaul could cost the organization significantly. If you are unable to effectively and clearly communicate technical issues and their impact on the organization to others within the organization they may not be able to understand what you are trying to tell them. And when they are not able to understand what you are talking about they may just 1. Disregard it, or 2. Not be fully persuaded that your issue is of importance to the company. When you are able to clearly communicate cyber security concepts and their importance/ potential impacts to the organization, those in power can make more informed decisions regarding security.

The final soft skill I think is important to practice as a cyber security professional is being able to remain calm and make difficult decisions under pressure. A job in cyber security can be extremely taxing and mentally at times especially in urgent situations. Not everybody is able to handle the pressure that comes with working in a cyber security field. If something falls through on the security side of things, it could badly reflect the public’s outlook on the organization. Along with this it may end up even reflecting badly on you, and even be carried with you for the rest of your career. This can affect the soft skill we discussed earlier about being trustworthy. If you react unreliably under pressure, your organization and future organizations you plan to work with may not find you a trustworthy individual anymore. When you are able to remain calm in stressful situations you will be setting an example and be seen as a leader in your work. Portraying negative emotions during stressful times can be contagious and if you display negative emotions towards others in your organization, it could lead to them becoming stressed out and not making optimal decisions either. Acting out of pure emotion in a cyber security position is extremely unprofessional. In one of our readings titled: ”What Makes A Good Leader? Key Differences Between Management And Leadership”, one of the key points listed as “Leaders Have Courage To Face What Others Fear”. In my opinion, this fits really well with being able to control your emotions. When you are able to take control of a situation instead of letting the situation control you, you are becoming a leader in that situation. And when you are able to act like a leader, others will respect and look up to you.

I think one of the biggest struggles I have when it comes to following my code of ethics is being able to make difficult decisions with large tradeoffs in an effective manner. As I talked about earlier, one thing that is not my strong suit is handling things like ethical dilemmas. Because I want to do what is best for both me and my organization I find it hard to purposely make a decision that will end in some sort of damage for either me or the organization. I will just need to remind myself that as I mentioned earlier in my code of ethics that the perfect security solution does not always exist.and that  It is important for me to seek opinions from multiple sources to gather an array of understandings. I will also need to remember that sometimes there will always be some form of trade-off when working in cyber security.

Before taking this class I did not really consider having a written out code of ethics to consult in times of stress. But after reading a few codes of ethics I can see why they are important in setting foundational rules and guidelines to help people make the right decisions when they live by their code of ethics.