Jonathon Schnell
April 6, 2020
CPR E 234x
Dr. Blakely
What is your personal code of professional ethics relating to your career in cyber security (i.e., the principles you'd be willing to resign or be fired before you violate)? How is this impacted by your personal values and the various considerations in the class? How might it change in the future? 2500 words.

Ethical dilemmas in the cybersecurity profession can become very murky very quickly. The primary cause of this is the rate of technological advancement. Every day a cybersecurity professional will face new ethically challenging decisions. These challenges are compounded by the fact that there is no universal and official cybersecurity body that has published a code of ethics for professionals to adhere to. This requires professionals to develop their own professional code of ethics from their personal code of ethics, person values, and personal background. The ethical principles that I strive to adhere to are. Do not cause unjust physical harm to another person or neglect the safety, health, or welfare of the public. Protect user's reasonable expectations of privacy. be honest and realistic, fully disclose vulnerability information, do not mislead clients or employees in any way. Seek and be open to honest criticism. Prioritize personal health over professional duties. Do not engage in corruption or insider trading, and disclose or avoid any conflicts of interest.Respect the law in all but the most extreme circumstances. Respect fellow employees and clients. Treat all people equally reguardless of race, religon, sex, disabilities, or sexual orientation.

All cybersecurity professionals should not, under any circumstances, cause direct or indirect unjust physical harm to another person, or neglect the safety, health, or welfare of the public. The idea of 'do no harm' is nothing new, as far back as the Greek physician Hippocrates medical practitioners have used this ethical principle as a pillar in their day to day practices. In my opinion there is no reason that cyber security professionals should not follow an ethical principle similar to the hippocratic oath.

The uptime of a computer system can cause real world disasters and loss of life. A prime example of this is in emergency services. If an emergency dispatch's system goes down there is a very good chance that it could cause loss of life. It is for this reason that I feel not that computer systems should be treated like a patient would be with regards to the hippocratic oath in medicine. In my opinion this ethical pillar is timeless, it's been around for almost two thousand years and I suspect it will be around for much longer than that.

I firmly believe that cybersecurity professionals should not partake in activity that violates the reasonable privacy expectations of any users, not just the users they have hired to protect. Privacy should be a huge concern to anyone pursuing a career in cybersecurity. This is again a result of the rapid advancement of technology. Rapidly developing analytical tools can extract more meaningful information out of less metadata than ever before. On top of that it is common knowledge that federal agencies have analyzed the metadata of innocent users in the past. This has increased the public awareness of a user's digital footprint and has caused users to be more careful about their personal details when using the web.

Jonathon Schnell
April 6, 2020
CPR E 234x
Dr. Blakely

Cybersecurity professions are obligated to protect company and client data from being leaked or farmed. This ethical pillar is worded carefully because as society changes users' expectations as to what is considered reasonable privacy change as well. Therefore this ethical pillar is also relatively timeless, only changing to match society's reasonable expectation of privacy.

Cybersecurity professionals should always be honest and realistic in claims, fully disclose vulnerability information, and avoid misleading clients or employees in any way. In my opinion honesty is a crucial ethical pillar in any profession, not just cybersecurity. However the cybersecurity profession is a technical field therefore it is very important that a professional understand the importance of not overstating claims to their abilities or the abilities of their products. It is crucial that when disclosing a vulnerability, it is done in coordination with the maintainers of the vulnerable systems. A good example of breaking this ethical guideline would be if a company were to disclose a competitor's vulnerabilities at an unsavory time to gain a business advantage.

To me, the importance of honesty stems from my religious upbringing. As a child and young adult I was taught to follow the ten commandments every sunday. The ninth commandment, from the lutheran scripture, states "Thou shalt not bear false witness against thy neighbour." I believe at its core honesty is a timeless ethical pillar for two reasons. Western society has upheld it since the conception of cristianity, and it is not unique to christianity. For example there is a jewish commandment, Negative Commandment 250, which forbids believers "from cheating each other in business when buying and selling."

In my opinion one of the reasons that technology is advancing so quickly is because technical professionals seek and are open to honest criticism. This ethical pillar comes from IEEE 7.8 Code of Ethics and without it we wouldn't be where we are today with technology. It's no secret that companies that listen to customers' feedback and adapt to the market are more successful than those who do not. Every new generation of technology must improve on the previous generation to create a better quality of life or even save lives. Improvement can only be measured relatively. For example this new computer is better than this old computer because it's faster, has more storage, and is more secure. These metrics are only valuable when compared with the old computer. The big idea is that it is impossible to improve upon tech without listening and adapting to feedback.

This ethical principle does not only apply to technology. For example a co-worker might give you constructive criticism about your presentation to the board could be more effective. You might do the same for your co-worker. If you're not getting better you're probably getting worse and if you're not listening to criticism you're going to have a hard time getting better. In my opinion this ethical value will hold just as much value today as it did yesterday, professionals should always be seeking improvement and the best way to improve is to listen to take advice from peers and clients.

Jonathon Schnell
April 6, 2020
CPR E 234x
Dr. Blakely

Careers in any technical field can be challenging and exhausting. That is why I believe that it is important to prioritize personal health over professional duties. The best example I can think of this is simple. Don't go to work if you think you are sick or have a fever. By going to work with a contagious virus or infection you risk getting your co-workers sick and creating a much bigger issue. A prime example of ‘a bigger issue’ is the current Coronavirus outbreak. All professionals should have a basic understanding of contagious viruses and how to avoid spreading them. A lesser known issue regarding personal health is burnout. Symptoms of burnout are lethargy, stress, and cynicism. Burnout is often caused by getting fixated on work to the point that it is detrimental to your social or mental health. If someone is burnt out they are more likely to make simple mistakes that could have serious consequences. This is why it is crucial that professionals put their personal health in front of their professional duties.

This is one ethical pillar that may change in the future maybe even the near future. I feel this way because the Coronavirus pandemic has forced many organizations to transition their operation from a traditional ‘face to face’ operation, to an entirely remote operation. Certain businesses may find the transition painful and unmanageable while others may find advantages to a remote operation. I suspect that some businesses will even adopt the remote operation strategy even after all shelter in place orders have been lifted.

Under no circumstances should a cybersecurity professional engage in corruption or insider trading, professionals should disclose or avoid all conflicts of interest. Corruption is a dishonest act that is committed by a person of authority. A prime example of corruption is bribery, that is to take money from someone in return for special treatment. Insider trading is another example of corruption. A cybersecurity professional might find themselves in possession of data that has not yet been made public, they should not under any circumstances use this information to gain an advantage when trading stocks. Typically corrupt acts are committed purposefully, the person(s) committing them know that what they are doing is wrong. A form of corruption that is less obvious is called a conflict of interest. A conflict of interest is when preference is given to family or friends in business. An example of a conflict of interest is if someone were to hire a family member over another applicant who is more qualified for the job.

Corruption is and always will be ethically wrong, but conflicts of interest might become more acceptable with society and time. Many cultures' ethical principles do not forbid conflicts of interest. For example in china it is not uncommon for professionals to give business preference to their family members. That is why I believe that it is possible that this ethical pillar might change over time to allow this type of behavior in certain circumstances.

Law and ethics are typically separate ideas because it is easy to conceive of a situation where it would in fact be ethical to break the law such as speeding to get a patient in critical condition to the hospital. With that being said I believe that all cybersecurity professionals should respect the law in all but the most extreme circumstances. Though a law may not directly translate to an ethical value, law can offer insight as to what types of behavior is acceptable. By following the law one is inherently following many ethical principles.This is why cyber security

Jonathon Schnell
April 6, 2020
CPR E 234x
Dr. Blakely
professionals should respect the law in all but the most extreme circumstances. A cybersecurity professional may be asked to launch a counterattack against an attacker which is currently illegal but may change in the near future[7]. Obviously laws are fluid meaning they change quite often but this ethical pillar is worded to include extreme cases where it might be ethical to break the law. In my opinion this pillar might change with time especially if the laws begin to become unreasonable or unethical themselves.

Respect fellow employees and clients. Treat all people equally reguardless of race, religon, sex, disabilities, or sexual orientation. Respect and equality are two massively important ethical pillars. My strong belief in them stems from my religious upbringing. In lutheranism the fourth commandment states “Honour thy father and thy mother.” While this commandment, in writing, only specifically talks about respecting ‘thy mother and father’, my pastor would preach about respecting all people regardless of reguardless of race, religon, sex, disabilities, or sexual orientation. As a US citizen I also draw inspiration for equality from the constitution of the United States of America, which states that “all men are created equally.” Respect and equality go hand in hand with the golden rule, treat others the way you would like to be treated. It is absolutely critical that all professionals treat all people equally and with respect because it has been said that respect is ‘a two way street’ meaning you have to give it to get it.

A prime example as to how one might violate respect is if that person were to engage in harassment of another employee or client. Harassment should not be tolerated in any professional work environment. An example of how equality can be violated is in employee pay. Two people with the same qualifications doing the same job should get equal pay. This unfortunately is not currently the case with women making around 95 cents on the dollar compared to men[6].

A less obvious breach of equality that a professional may experience ties back to the privacy argument I previously made. Imagine being tasked with writing an AI model to be used for determining if inmates should be let out on parole. The main idea is to determine an inmate’s likelihood that he or she will reoffend. The problem comes if you use prejudice data to train your model. In this case the code will also behave with prejudice. Whose fault is it if it is found that the model makes prejudiced decisions in deciding a humans worthiness to be free.

With all of that being said the ethical principles of respect and equality have been preached for over two thousand years. I see no reason why they would not survive another two thousand years time with little change. In my opinion respect is key to the survival of any advanced society and is a building block upon which almost all other ethical principles are based.

Cybersecurity is a young and rapidly developing career field with no clearly defined code of ethics in place. This creates a challenge for professionals to develop their own professional code of ethics from personal values, and personal beliefs. My professional code of ethics, developed from my personal beliefs and various considerations discussed in Cyber E 234x, is as follows. Do no harm, Protect privacy, be honest, Seek and be open to honest criticism,

Jonathon Schnell
April 6, 2020
CPR E 234x
Dr. Blakely
prioritize personal health, do not engage in corruption, respect the law in all but the most extreme circumstances, respect fellow employees and clients, and treat all people equally reguardless of race, religon, sex, disabilities, or sexual orientation. My personal goal is to follow these ethical principles not only through my cyber security career but throughout my life.

Works Cited :

1. https://www.chabad.org/library/article_cdo/aid/961882/jewish/Negative-Commandment-250.htm
2. https://10commandments.biz/biz/ten_commandments_list_lutheran.html
3. https://www.britannica.com/biography/Hippocrates
4. https://www.ieee.org/about/corporate/governance/p7-8.html
5. https://www.psychologytoday.com/us/blog/high-octane-women/201311/the-tell-tale-signs-burnout-do-you-have-them
6. https://www.payscale.com/data/gender-pay-gap
7. https://www.infosecurity-magazine.com/magazine-features/search-ethical-code-cybersecurity/
8. https://towardsdatascience.com/the-hidden-dangers-in-algorithmic-decision-making-27722d716a49
9. https://www.biblegateway.com/passage/?search=John+13%3A34-35&version=NIV