Trevor Kems
CPR E 234X
May 1st, 2020
Dr. Blakely

Personal Ethics

Ethics in cyber security is something that at most times seems intangible. However, I feel that certain aspects of that intangibility only seem that way due to future uncertainty. This class has taught me many different ways of thinking about ethics in the ever changing world of cyber security and information technology. It also gave me the ability to make my own choices in regards to example ethical problems, just as one would in a real life decision.

Cyber security is full of problems and most of them result from some sort of ethical issue. When thinking about cyber security, the public likes to think of movie style hacking scenes or government actors tracing phone SIM cards using MySQL injection. However, industry professionals laugh at these scenes due to them being very different from the daily routine. The daily life of a cyber security professional could range from simple updates to computers to responding to an attack on the main server that causes multi-million dollar losses for the company. However, hidden in most, if not all, of these problems is usually an ethical dilemma that cyber security professionals must face head on. For example, if a staff member has not updated their computer for many months as they have evidence from others it will break a piece of software they use everyday, it can be an ethical challenge whether or not to allow their computer to fall behind on updates in order for them to be able to keep using the software that they are familiar with. What about the next employee who overheard your conversation and then never updates their computer? This can lead down a rabbithole of problems. However, I think that this is one ethical issue that I think some professionals would be able to solve quickly. I personally have the opinion that machines should be updated as regularly as possible and should only be left out of date if there is a plan in place to move to a different system that is up-to-date. But others may think that it's okay most of the time. This simple ethical dilemma can cause headaches for future professionals if not handled properly.

While I'm sure that most cyber security professionals would love to deal with simple update questions every day, there are more complex ethical problems that come up from time to time. One such example is that of employee separation. When an employee leaves a company it can be for many reasons. Termination, moving employers, or moving to a different area are all common reasons an employee would leave a company. The ethical issues arise when the personal connection to an employee can create issues with the separation. This is common when an IT related staff member is terminated who had a personal connection to the IT staff. Giving special treatment to the staff member during termination can lead to issues such as loss of data such as intellectual property, theft, or abuse of company systems. These can all come from not following company procedure, or not having the correct procedure, when dealing with former employees. An example of this would be of an IT staff member that is very close to the lead cyber security manager. When the IT staff member is let go due to budget cuts, the former IT staff member asks the lead cyber security manager to keep his company email and file server

account active for longer than normal due to the amount of personal information stored on the company system. While this may seem like a harmless request, the cyber security manager has to worry about the company before a former employee. I believe that the cyber security manager should not grant this request as it can cause issues with handling sensitive company data. The former employee may want to get revenge on the company by stealing data and giving it to a competitor. While this decision may seem like a simple one, it becomes more complex if a friendship is involved with that former employee. My personal code of ethics would always put the company first when friendships are on the line. This will protect the current employee (myself) and a former employee of getting accused of any wrongdoing. This is just one example of how friendships can cause many issues within the information technology and business world.

Another side of ethics in the information technology world is that of intellectual property. While digital rights management, or DRM [1], is found in many devices and software today, it still does not prevent all forms of priacy. I feel that anyone with at least a medium level of skill with technology has heard of and knows how to procure pirated software, music, or movies. This brings up an important point, is priacy ethical? My personal answers are sometimes, but business related answers are always no. While most people would answer a simple yes or no, I feel that most of the time there is more depth to why someone pirates certain types of media. It can be due to cost, obscurity, availability, censorship, or many other reasons. I personally think that piracy is overall a bad thing, it steals intellectual property from others without payment. However, in certain cases, piracy can be a good thing. In the United States and most of the world, the copyright system, in my opinion, is broken. It allows people and corporations to keep works locked up for decades even when they have fallen out of use years ago. This is a problem for archiving, sharing, and collecting older media. A good example of this would be vintage computer collectors. Being one of them, I should state that this may be a bit biased. Finding software for multi-decade old computers is hard. Due to the lack of internet, many of these machines do not have original software or backup disks used to restore the computer in case of failure. I believe that older software or media can be pirated when there is no other source for it due to age. While I understand the argument against mine in terms of intellectual property, I do not understand how decades old software that is no longer being sold or marketed as having value to the original creator. In the business side of piracy, it is never, in my opinion, okay to pirate software. Businesses have more of a responsibility to keep their software up-to-date and licensed than individuals as more people are dependent on it. Piracy also can affect a business more and does not have anything to do with archiving or finding outdated software most of the time. This is why personal and business piracy are separate in my view.

Due to how broken the copyright system is for personal use, I feel that patent law is a better example of how an intellectual property system should work. Patents are protected for up to 20 years [2] with optional extensions. This system allows for up to two decades of use by the

original creator before being allowed use by the general public, which in my opinion is enough in most cases to allow for the original inventor to make money off their invention. If the same is applied to copyright, a 20 year old piece of software is most likely not going to be making the original creator much money due to how quickly computers age and update. Therefore, this would allow collectors and hobbyists the ability to tinker and change older software or archivists to save computing history. This is why I think that ethically, piracy is sometimes okay in order to fill the incorrect and outdated law that is currently in place.

The ethics in cyber security cause many decisions to become difficult to make as they can comprise friendships or cost you your job. One example of the latter would be that of an unethical decision made by a supervisor. On one hand you could lose your job if you do not 'follow orders' and on the other you could be causing the company to have security issues and possibly causing data loss. This becomes a hard choice to make for even the most seasoned cyber security professionals. Because of how external factors such as the current job market or if you have a family to provide for, this can go either way. Ethically, I feel that going against a supervisor can cause issues in your work environment for even small things. However, I think it is also important to think of how to correctly handle security problems regardless of a supervisor's opinion. As discussed in class, the best way to correct a problem is to come to your boss with a solution. This applies to both problems that you have and have not created. Therefore, I feel that if someone is in the position to go against a supervisor's orders to decrease security, they should. However, if they are unable to at the moment due to factors outside of their control, such as family life or job security issues, they should be planning to move as soon as possible and also log what decisions they have in order to hopefully not get burned by the company later.

Ethics are very individualized which can cause problems within teams. However, most people have similar ethics when it comes to security. This sometimes can not be true when someone has incorrect information or other problems such as budget constraints. Most people feel that security is important until the cost breakdown is shown and they decide to shrink it as much as possible. As stated in the last paragraph, getting burned by your employer for bad security could be very bad for someone's reputation. For example, Equifax lost millions of customer records which included social security numbers of over half of the American workforce. A decision that was made by a supervisor, implemented by you that cost millions of Americans their social security numbers could ruin your reputation in the security industry if it was found that you just followed the direction of your supervisor and did not speak up when you knew that there was a security problem. Therefore, it is important to have multiple people with multiple different sets of ethics review security changes. This is often an outside auditor that has no stake in the company itself and only does security reviews, but it also could be a well funded security team that reviews the company and is able to bring security issues to light without fear

of removal. This balancing of ethics allows for more security but does increase cost. This is the primary reason, I feel, that companies will not take security more seriously. The bare minimum is good enough for most companies, even if they need more.

My ethics in cyber security are very grounded in my personal experience. As a young pre-teen, I learned about computers from just messing around with them. I always wanted the best computer but had to settle with whatever second hand computers my Dad brought home from work. I learned to tinker and use the internet to my advantage to try and work everything I could get out of those sometimes decade old computers. I also remember being taught to not do bad things. I am lucky to have good role model parents who taught me to do things the right way the first time to prevent having to be embarrassed or having to do it a second time. I also hold myself to a high moral character. These things that I was taught when I was younger helped me get into security safely. I did not start in security with the idea of hacking computers in mind, I got into it as a way to prevent the 'bad guys' from getting into your own computer systems. The first security lesson I got was from the IT Olympics and the High School level CDC. This allowed me to be able to learn about security safely and have fun while doing it. I learned so much every year for four years that I decided that it would be a good idea to make this at least a focus in my higher education. Little did I know during my first few CDCs that I would be doing the college level ones only a mile away less than five years later with a brand new major that had a focus in security. While back in high school, I knew that the things that I was doing could be used for bad, but I just had the gut reaction to only use them for good. I guess that was in part from my upbringings and the role models I had, but I feel that the ethics involved also came from learning how things worked and not wanting someone else in my own system.

During the class, ethics was something I thought about constantly. Even in topics where ethics was not the main point, ethics was always in the back of my mind. For example, during the talk about power infrastructure at Mid American Energy, I caught myself thinking about how ethics would be very important in protecting the North American power grid. One wrong move by an employee or incorrect decision by a supervisor could cause people all over the country to lose power for days at a time. Therefore, proper ethics are required for employees to question their supervisors when it comes to hard decisions. Also during the class I found myself thinking about government positions. Ethics can be a hard pill to swallow when national security is at stake. I think of Edward Snowden in this case as he used his personally gained ethics to decide when to leak government documents to the media about NSA spying. This, however, caused him to become an outcast from American society. However, I think he taught the American people about how to protect our data and not allow government overreach as much as possible. A government job where classified information is important is something that should not be discounted, however, ethics sometimes have to be put aside when working in an atmosphere such

as that. National security sometimes is important enough where ethics can be overridden, however, some ethics can not be overridden.

For the future I know that ethics will play a huge role in how I work with others and how I deal with problems. Certain ethical problems are simple, such as the computer update example, but some are hard, such as going against a supervisor's requests. These problems are hard to think about ahead of time due to their ever changing nature and the outside forces that cause them to happen. However, I feel that my upbringings will allow me keep a straight moral and ethical compass and allow me to work around issues that are thrown at me. I also know that whatever ethical dilemma occurs, I can think back to CPR E 234X and think about our discussions and what ethics mean to other cyber security professionals that are in the same position I am in. Therefore, I feel that I am well prepared to go into the workforce and continue keeping ethics as a top priority.

Sources:

1. https://en.wikipedia.org/wiki/Digital_rights_management
2. https://www.uspto.gov/help/patent-help#patents