Trevor Abel

Professor Julie Henderson

CSCI 325

3 October 2019

Confidentiality of Information in Cyber Security

Ethical issues have been soaring to the top of the cyber security filed lately with more frequent whistleblowers and after the rise of Edward Snowden. Through that single whistleblowers' actions, it sparked an interest into the actions of all cyber security and systems analysis jobs. Through the analyzation of the actions that they used several problems became apparent or things were identified that could become problems. Two of those are confidentiality of information when someone is hired to go in and analyze a system for security purposes. As well as hacking within the community. Within the ethical bounds of access and defining what areas are legally accessible there is still a large grey area about how that information should be handled and this paper will explore that.

Confidentiality is a large topic issue within the cyber security community due to the simple fact that companies out-source for system analysis. This is because they can think of maneuvers to try that someone working within that company would not try. When companies invite these people to analyze their systems the define where to search and then they legally have access to all those files within their areas. In this area is where problems can arise because this job is built on "the principle of keeping secure and secret" information that a cyber professional has access to (Kelley and McKenzie). This can be both easy and hard to maintain because as a professional your focus is on your work and keeping your job so it would be easy to disregard the information you may encounter. However, it can be hard when files or information does not

appear beneficial for the company's name and can lead to doing some digging within the system they are working on. Another issue within this is that some companies will let cyber professionals use their own devices for analysis of their systems. This is a bad practice because this allows the professional to be able to take files and leave with them on their machine making it easier to take files than it should be from a company with information to protect. In this area we see a lot of gray room for cyber professionals to operate as they choose some companies will even go as far as giving them full access to their systems for analysis. This can become and issue especially when dealing with classified or sensitive information because it can be taken easily.

Even if the information is not taken it can be just as bad because if some system files reveal that a company is involved in some malicious practice or bad dealings then if it leaks that they have files about this they can get into legal trouble. However, if confidentiality is something that a cyber professional is providing then the point at which to draw the line to report data is at best extremely blurry and sometimes not even drawn out. This leaves a lot of decision up to the person performing the examination and leaving that much power in the hands of one person has not proven to be great for companies. Even when someone is required to use a provided machine with intranet that is filtered and monitored we see that "Intranets may provide a false sense of security" this can be dangerous (Kelley and McKenzie). This is bad because if a person has malicious intent going into a job like this then they can cause all the damage they want just through a small series of attacks because intranet is also extremely vulnerable.

Another issue within the cyber security community hacking and it ties into confidentiality because anyone now with the right certifications can pose as a systems analysis person and provide some form of support to a company. This is a problem because people who know how to hack into systems, black hat hackers, can easily pose as people who are only trying to protect

data so that they can steal the data. White hat hackers are people who want to protect the data and make sure that nobody can take it and use it for blackmail or sell it. The main jobs for these people are “attempt to find security holes via hacking” and this is the proper way to utilize hacking so that information does not get leaked (Norton). While on the other side there is a group of people with malicious intent called black hat hackers and they aim to take information. The problem in this is neither one of these terms are solid its all situation based because a person can turn in an instant to a black hat hacker even if they had no intention of it. This issue is big because if the person feels like they are not being treated well enough or being payed enough and they have access to sensitive files they can easily take them and use them against the company they were hired by for blackmail. Dealing with a black hat hacker is hard because they know how to cover themselves and they attack in a “range from simple Malware spreading to complex vulnerability exploitation and data theft” this makes them unpredictable and dangerous to people and their personal information (Townsend).

I believe that to overcome these dilemmas in the cyber security field it is very important to have all specified areas laid out on paper as to what needs to be inspected and some form of accountability or supervision is a great idea. This helps keep people honest in a time when it is easy to take information in these circumstances. I also believe it is important to decide what works best for you and work with the company to make sure that you have the safest ethical setting for both the person as the tester and the company for their information. This is important because it sets strong and defined boundaries which makes it harder for someone to claim that it was never expressed that they could not access a certain area. This helps hold you accountable and will be a good guide for a professional career because it sets a high standard for your work

ethic and puts boundaries that can help you avoid potentially compromising situations that would be bad for your reputation and job.

I feel that I need to work on structuring definition so that if and when circumstances arise I can be able to walk away to protect my integrity and my reputation. Other than that I feel that I am ready to face these challenges because I know that accessing areas that I would not be permitted to caries a huge penalty and I do not want to worry about that in my future. I feel that I have set my mind to avoid any situation that would put me in a compromising situation because I would want to continue doing this line of work and that would prevent me from fulfilling that.

Works Cited

Kelley, Grant and Bruce McKenzie. *Security, privacy, and confidentiality issues on the Internet*. 22 November 2002. 3 October 2019.

Norton. *What is the Difference Between Black, White and Grey Hat Hackers?* 2019. 3 October 2019.

Townsend, Caleb. *What is the Difference Between a White Hat Hacker and Black Hat Hacker? | United States Cybersecurity Magazine*. April 2019. 3 October 2019.