**Miller, Ryan (693119) 1/29/2022**

# Section 1: Protecting Against the Danger From Within: How Digital Forensics Can Identify Insider Threats Executive Summary

There is a rise of internal cyber attacks with ransomware within the past few years. This means that there are people inside businesses who are attacking the companies and the companies can lose a lot of money: between 11 million to 13 million dollars on average. This causes companies to take actions to increase their defenses and responses to these attacks. It is almost impossible to prevent these attacks because of all of the different ways a company can be assaulted. One of the ways the companies have come up with resisting these attacks is implementing tracking software to be able to easily find out what employee attacked them, when and where the attack occurred. While this doesn’t prevent the attacks it can help minimize employee’s motivation to attack. This digital forensic software will also provide information on how they were attacked so that the cybersecurity team can put into place a defense in that area.

There can be multiple kinds of attacks. If the attacker goes after the IP, the forensic software can be used find out what file was leaked and what was done with it so that way the company can have undeniable proof of what happened, and it can be provable in court. There can also be leaks through twitter, which then they will use the timestamp of the post and then track down where they moved the file too, if through email or external USB drive. If the employee isn’t smart enough, they may even use their own work computer, which will have records of everything which is strong proof against the attacker. Every piece of data that the forensic software can find will be able to be used to help prevent these kinds of attacks in the future and provide evidence for termination and lawsuits in court.

With all these attacks becoming more common, police departments need to increase their resources in the cyber communication section. It is believed that “90 percent of crime has a digital element.” However, because data can be easily manipulated, the tools that were used to find the data for prosecuting the employee have to be examined because the tool has to be correct, because if it isn’t the court will throw out the case. Strong forensic software will help reduce the weight on the police department and expedite the termination and possible lawsuits against the employee.

Cybercriminals are becoming more and more common and stronger. Cybersecurity teams must stay vigilant and continue to improve their prevention software to stop more attacks on their company.

# Section 2: Personal Reflection

This article brought up some interesting thoughts for me that I have never considered. Cyber security is way more important and more complex than I had ever considered. The detail and how thorough the program is needs to be very complete. If there is one little gap inside the forensic software, hackers or employees could abuse that hole and make a lot of money and hurt the company a lot by doing so.

One of the things I also liked learning about was all of the different kinds of ways the forensic software can track and learn about the criminals’ movements. From following just a simple time stamp on twitter to following their specific IP address and learning what was done with the document.

The final thing that I found very interesting was how thorough the program needs to be, because of the need for proof. Developing that kind of software has to be very involved with a lot of testing so that the data is actually able to be used in court.

One of the thoughts that came up in my head is actually if I would want to go into the cybersecurity business. I think it would be an exciting opportunity to learn about how people try to hack companies’ software and then do my best to be able to actually prevent any sort of attack from outside or from the inside.

# Section 3: Questions

* My first question is what kind of meetings does each team member need to go through so that they can understand the importance of being safe and not allowing hackers to get in?
* I would ask the author to clarify how much evidence is needed for the forensic software to come up with to be actually provable without a doubt in court.
* My final question would be how much does the employee benefit from defecting and attacking their current company?

# Section 4: Personal Application

One change I will make in my life is to investigate if I should become part of the cybersecurity world with my degree or if I should continue on my path of trying to become a video game developer. I will research for an hour once a week to learn about the cybersecurity world and if it seems just as interesting as I think it is now.