NAME: Megan Leonard

TODAY’S DATE: 2/5/2023

# ISEC 375 Homework 2

Answer the following questions based on your reading of the textbook, the module key points, and the instructor’s presentation this week.

1. **[6 points]** You are assigned to set up a forensic lab. The lab’s primary objective is to conduct investigations involving industrial espionage and national security cases. You don’t have a budget problem. What personal and physical security precautions would you expect to see in your lab?

Without having to worry about a budget, the first necessity is that the room that is to be the lab, does not have any windows. The door needs to be able to lock and be thick enough, same with the walls, that a person can not just break it down. The screws of the door should be located on the inside so it can not be unscrewed by someone outside the lab. The data needs to be able to be stored in a secure container whether that is a thick safe or a storage room with thick walls and door with more locking mechanisms. I also expect to see stations set up with the only ones having internet access being the ones used solely to look things up. There is also a physical log that is written when someone enters and exits and a sensor on the lab door to indicate when it has been opened so that times can be matched up as needed. For personal security, the staff would know about the security policies so they do not end up blind sided by something they may not know like not knowing they have to sign the log when leaving as well as entering. There will also be badges that the staff needs to always wear and must report it should it go missing so that security can remove the clearance of that badge should the badge itself be used to gain entry.

1. **[6 points]** Specify at least three factors that help a lab manager in prioritizing hardware and software procurement for his/her lab in a private company?

The first factor that helps with the prioritization is the financial amount that is available and the cost benefit analysis of the different hardware and software. The second factor is what the staff members have training in and experience for example, if all the computer systems are mac but the staff only knows windows then they could make mistakes as they are now learning how to work with this other system. The third factor is what the lab will be working on itself for example, if the lab is small and only working with smaller data and devices, they may not need a giant safe when a smaller one would work better.

1. **[6 points]** What is the purpose of a lab audit? Please give three non-conformities you may come across in a lab audit?

The purpose of a lab audit is to make sure that everything is running up to code within the lab, making sure the work is secure and the people themselves are safe. A non-conformity that may appear during an audit is that the data is not being stored in secure locations and containers, like if the workers are leaving for the day while leaving the devices they are working on just on their tables. Another would be the workers either not getting or not taking their mandatory breaks as these are important for the employees’ health and their work as they can not work to the best of their ability if they are tired from long hours or hungry. A third non-conformity is that the lab is not following the room rules such as having full walls and a secure room without windows.

1. **[3 points]** What is the significant difference between the forensics labs of a police department in a major city and a big enterprise?

The significant difference between a police force and a big enterprise lab is the type of investigation tools they keep. For example, the police could be gathering evidence from a person only to find that they use a computer from the 90s and floppy discs. The police lab would have to be able to run the floppy discs to check them as they could hold important data. The big enterprise lab would be very unlikely to work with floppy discs and would instead focus on the technology they have at work, more used devices like flash drives or CDs.

1. **[3 points]** What are the benefits of using a disaster recovery plan for a forensics lab?

The disaster recovery plan is a means of preparation for future problems. Having one gives the benefit of being prepared for these events as to keep from panicking and can help restore the workstations and files into their original condition as you may lose work but not everything.

1. **[6 points]** You are working as a cybersecurity analyst in a large energy company. Because of the high frequency of the cyber-attacks against your company networks, you are assigned to build a business case for an internal forensic lab by your department manager. What do you do to get upper management approval with no/minimal revisions to the plan?

The first step I would take is to write out the reason why the lab is important in the first place. To be able to have the lab be considered, upper management needs to see that there is a reason for it to be implemented. Along with the why, we can put amount of time and cost it takes to go against these cyber-attacks as this is something that is frequent. By seeing that they are loosing money while the attacks are being dealt with and the damage that the attacks have done they can understand the reason for the lab. To start with the lab, we can show a cost benefit analysis as to how the lab will save money compared to any lawsuits or any downtime that must be taken because of these attacks. Next, we go over the necessities that would come with the lab and compare the short term price of the lab creation to the long term loss that we would see without it. We can then show that long term costs for the lab would be less compared to without. The items will be shown with how they are to be used with the lab and the benefit each item has to show that each item will be used and are not an excess expense. There would also be the timeline of when the lab would be running, when different items will arrive and be put into use as they come in. We would follow this with showing a skeleton list of security policies that would be used with the lab to show that the sensitive information will be handled in a proper and secure manner. Finally, we would show them a planned schedule of inspections and how the lab inspections would work. Overall, I would want to cover the why we need it, how it can be implemented, the benefits of it, and the security that would be used for the lab and the expense at the different areas.