Journal Entry #4 & #5

November 7, 2021

1. **What are the costs and benefits of developing cybersecurity programs in business?**

It is certainly a must to have some sort of cyber security operation connected to any business. Whether that be an in-house team or a third-party company, securing confidential information is of upmost priority. Having secure systems allows businesses to reach their goals to protect the integrity and availability of information. This of course comes at a cost. For starters, hiring a cyber security team is a huge cost. Then after that there is the cost of all the equipment for the team. There would also be the need to develop a strong security policy. It is also important that the software used is maintained and updated frequently. As you can see there is a lot of labor costs into developing a cyber security team. Another note that should be added is that all other employees need to be trained as well and that is another cost. All of this is going to cost a lot of money however, the cost outweighs the potential amount that can be lost without a cyber security program. Last year the U.S had the highest average losses of $15 million per company due to cyber-attacks. These attacks cause organizations to cover things like detections costs, investigation costs, containment costs and recovery costs. So it is advantageous for companies to have strong cyber security programs in order to keep their data safe and keep cyber-attacks at minimum.

2. **How can you tell if your computer is safe?**

Keeping your computer safe requires you to be proactive. First, it is important to have a good anti-virus software running on your computer. This software is used to prevent, detect, and remove any malware injected onto your device. Another safeguard is to have a firewall setup. A firewall has the capability to preserve both software and hardware on a network. It prevents malicious software from entering your system. It is also important to have a physical backup of all your data on another hard drive. This is to be used in the event something does happen and you lose all your information. It should be backed up frequently to keep the most up to date data. Nothing is impenetrable as there are always going to be vulnerabilities but with these steps, your computer will be a lot safer than without. Adding more friction to the ability of hacking systems can prevent hackers from trying to attack you. The more obstacles in their way, the more likely they are to be annoyed and move onto the next one.