## WEEK 9 ASSIGNMENT

Chapter 10

**1. In what ways is denial of service (lack of availability for authorized users) a vulnerability to users of single-user personal computers?**

- The main vulnerability is that it opens up the service for massive amounts of requests that can be sent to the servers and then at key moments overwhelm it and therefore not allow actual users in. This is common practice for many hackers when they want to block information or access to one system while trying to gain access to another connected system.

- People who are on a single computer can be completely blocked by this because their single request is there only access point and with that one request, they have no access if it is blocked.

**2. What is the value of your own personal computer? How did you derive that number? Does it cover the cost to recover or recreate all the data you have on it?**

- I estimated the value of my devices by taking their original cost and then comparing that to current market value of similar devices. Since I take care of mine more than others and some of my devices are custom like my desktop or laptop the price can fluctuate. Also, since the current market for graphics cards is overvalued the value of my desktop is higher than it was 2 years ago.

- Currently the values of my devices do not have anything to do with what is stored on them. All of my important data like files that I couldn't recreate are backed up somewhere else on other devices or on other storage services. This allows me to recreate the device if needed but I would most likely take that opportunity to upgrade since recreating tech of any kind after its 2-5 years old is pointless.

- I don't want to calculate the current value of my desktop because it will just show how much it has depreciated in the years since I bought all the components; and therefore, how much money I have lost :P

**3. Investigate your college/university's security plan or an employer's security plan to determine whether its security requirements meet all the conditions listed in this chapter. List any that do not. When was the plan written? When was it last reviewed and updated?**

- My companies current security plan is actually very good since we have to meet the requirements of many of our clients that range from Intel to smaller organizations. Therefore, many of the elements that are described in the chapter like having policy, current state, requirements, and scheduled maintenance are a must have since the customers will require it to be handed over in negotiation. The levels of access and types of resources that we have are included along with statements of how our security resources are used.

- Along with this the "plan" that we have is ever changing. I know for a fact that it was recently changed since we just got a new head of IT and some internal system and software were changed along with that. Although we are on the right track now our IT department is actually not that old, so I’ll say the original plan was constructed about 6 years ago.

**4. For a bank, what are its most important assets? What are the minimal computing resources it would need to continue business for a limited period (up to 2 days)? What other systems or processes could it use during the period of a disaster?**

- For a bank, which is presumably large, there are two important assets in security: a continuous plan for improvement/updating and a recovery plan when something fails. Then there are the obvious assets like hardware, software, documentation and data.

- With a recovery plan there should be regular backups implemented of all important electronic data. This would preserve the banks critical information that it needs in order to continue business.

- Having a continuous plan for improvement/updating allows people to know a level of the system that could change their perception of the system and how it works but most importantly it denotes what needs to happen. Knowing what is going to happen in the future or rather what should happen in the future allows for even better planning and even improvement upon that original plan.

- The minimal resources that a bank would need to continue business is access to its data, and in order to access that data you would also need a system with the right software.

**5. When is an incident over? That is, what factors influence whether to continue the work of the incident handling team or to disband it?**

- An incident has concluded when it has been identified and then handled effectively, which is subjective to the environment. For instance, some environments wouldn't require investigation into the functional impact of the incident or the information impact. Often time the most important factors to think of are: what will this incident mean for the current usefulness of the impacted system, and what will it mean for the future of the impacted system.

- Depending on the system more or less investigation into the incident may be required. For instance, if the system stores data that has a layer of secrecy or rather the data is not secret but changing it in some way can have large impact.

- Know the information above is critical in the planning of how to deal with the incident and possibly fix an error or flaw in the system.