Unit 6 Critical Thinking Questions

1. **With Cybersecurity, better protecting the digital landscape can be done by putting yourself in the shoes of people trying to harm it, like black hat hackers. What other industries or businesses may benefit from the same kind of backwards approach? For example, could banks be better secured if we designed them while peering into the mind of a bank robber? Come up with another example like this and use it to evaluate this concept.**

Anybody can benefit from this. This really helps to improve security, as since you're thinking like them, you can try to figure out how they will attack. By finding that out, you can take the steps to block those ways so that black hats can't get in. For example, this would help the Energy/Utilities industry be more protected from people who want to shut them down and demand a ransom for operations to continue again.

Now there is the risk of people turning over to the other side, but there is no **perfect** way to do anything in this field.

2. **The best way to model threats against computer systems is to step into the criminal's shoes, adopt their mindset, and consider all the different ways they might attack. But how might doing this be problematic or lead to negative consequences? (Think white hats going over to the dark side).**

This could be bad because then people may get into the mindset of black hat hacking through this modeling, and then jump over from the white hat side to the black hat side.

3. **What is the first step a successful hacker is most likely to perform as part of their attack on a system? How can knowing and understanding this step be useful for a white hat hacker, and what can they do to use this information to stop a black hat hacker from even getting through the first step of an attack? Explain.**

The first step they will perform is their **reconnaissance**. This is where the attacker(s) identify their target and figure out the strengths and weaknesses of the system to develop an attack plan. Knowing this step can be useful for white hat hackers because It can actually be beneficial. Since white hat hackers help improve systems, doing this tests the security of the system, and changes can be made from that to better improve it. This helps to make the entry points for black hat hackers even narrower.

4. **Consider the possible responses to perceived risk listed in the unit. Which of these do you think is most frequently used? Why? Which do you believe would be the most difficult to employ and why? Explain.**

Risk assessment I think is one of the most used responses. Assessing what may possibly happen is a very efficient way to determine what actions need to be taken for protection. Not knowing what may happen will make it harder to make an efficient protection plan. The most difficult one to employ is **threat modeling**. It is a very useful thing, but can be difficult to develop as you may not know every single component of the possible risk. This means you won't get a fully modeled threat.

5. **One of the possible responses to a perceived risk is to mitigate it. What exactly does this mean? Do a bit of online research into the various mitigation strategies. How could you appropriately conduct one of these mitigation strategies in the face of a possible risk?**

"Risk mitigation strategies are designed to eliminate, reduce or control the impact of known risks intrinsic with a specified undertaking, prior to any injury or fiasco" (River Logic). Examples include prioritizing cybersecurity risks, implementing a cybersecurity framework, and train employees to follow a plan. Having a plan set in place is a very good thing to do. So if you see a possible risk on the horizon, you can implement the plan to make sure nothing goes wrong with this possible risk.