**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 5**

Names of team members: William Brown, John Hopson, Taylor Payne, & Corey Cooley

Logistics

A. Get into your regular team

B. Discuss and complete the assignment together. Don’t just assign different problems to each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

**Problem 1**

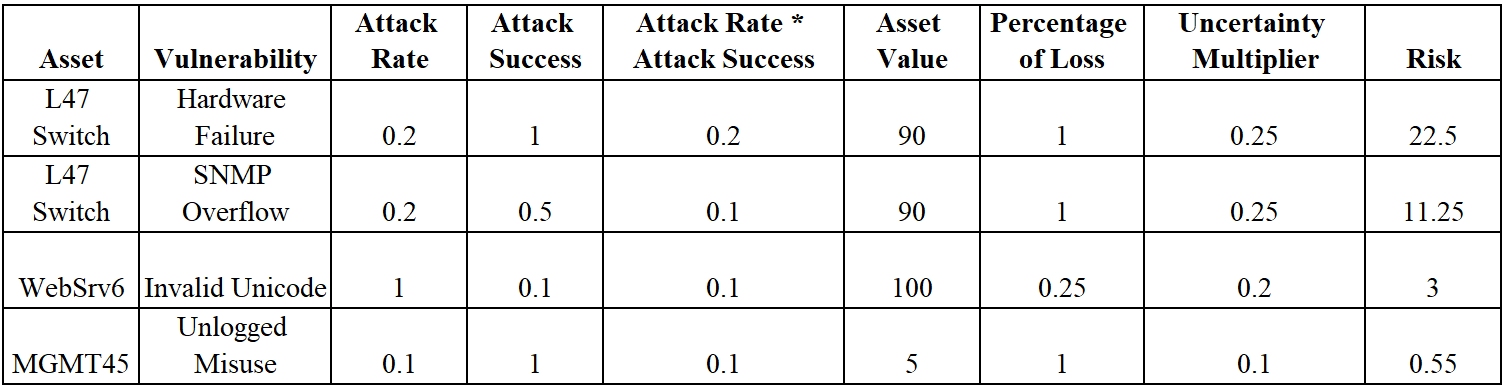
Complete Exercise 1 from pp. 320 of your text with the following changes. Switch L47’s hardware failure has an expected rate of occurrence of once every 5 years and when that happens it is 100% failure of the device.

The SNMP buffer overflow has an expected rate of occurrence of once every five years but only 50% of those attacks are successful. When it is successful, 100% of the asset would be lost or compromised.

For server WebSrv6, the invalid Unicode vulnerability is attempted to be exploited once a year but only 10% of those attacks are successful. When those attacks succeed, existing controls keep the loss down to 25% of the asset.

For the MGMT45 console, the estimated rate of occurrence of unlogged misuse by the operators is once every 10 years but when it happens, there are no controls in place to reduce the impact, so 100% loss of the asset is likely.

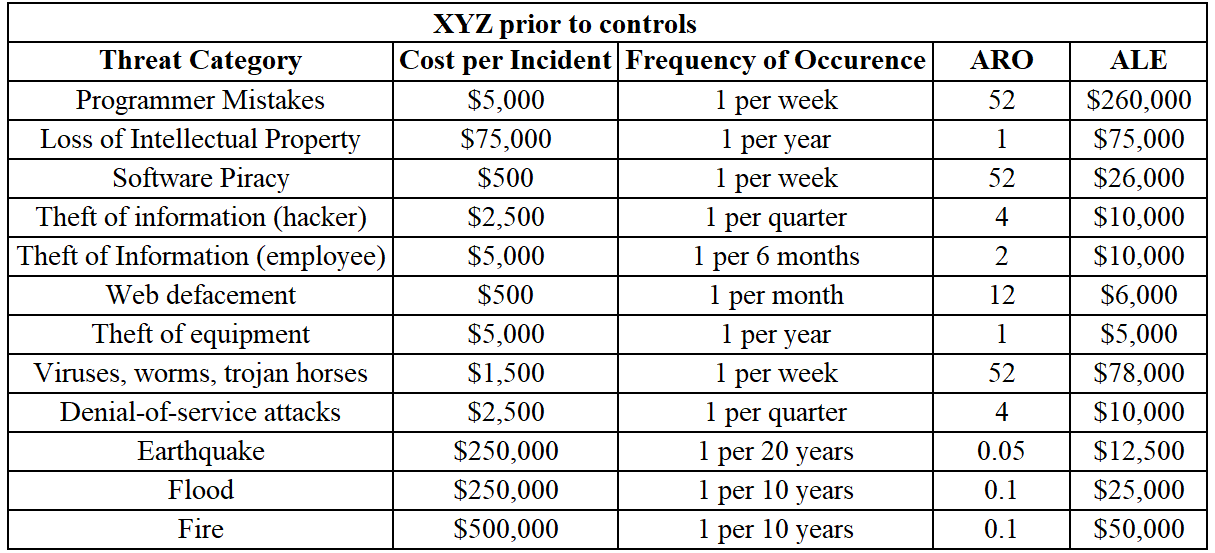
Perform the risk calculations (as shown on p. 287) and determine in what order these vulnerabilities should be addressed based on relative risk. Show your work. (15 pts.)



1. *High risk: L47 Switch shows the hardware failure will be a total failure with few remaining parts able to be reused. Even though occurrence is low, the switch causes a 100% loss. This should be evaluated first for additional controls such as insurance. With the risk of 22.5%, this is our highest risk threat.*
2. *Medium Risk: L47 holds the medium risk with the SNMP overflow. Most likely a control like a software update could help, but only in the case of this overflow. The switch is 100% loss, and depending on if there is a better defense strategy available, either update or get rid of the equipment would be the best options. This risk is another high risk threat.*
3. *WebSrv6 has a low risk, but an impact value of 100 points making it an important part of the system. The impact to profitability is high and a switch in this category can lead to stoppage of revenue or operational activities. With the a risk of 3, this is a low risk threat.*
4. *MGMT45 has a miniscule risk, and an impact value of 5. The impact would be stalled productivity or potential stalled operational activities from unlogged misuse. Controls could be potentially put into place to mitigate misuse, such as passwords and log files to track user interactions with the system.*

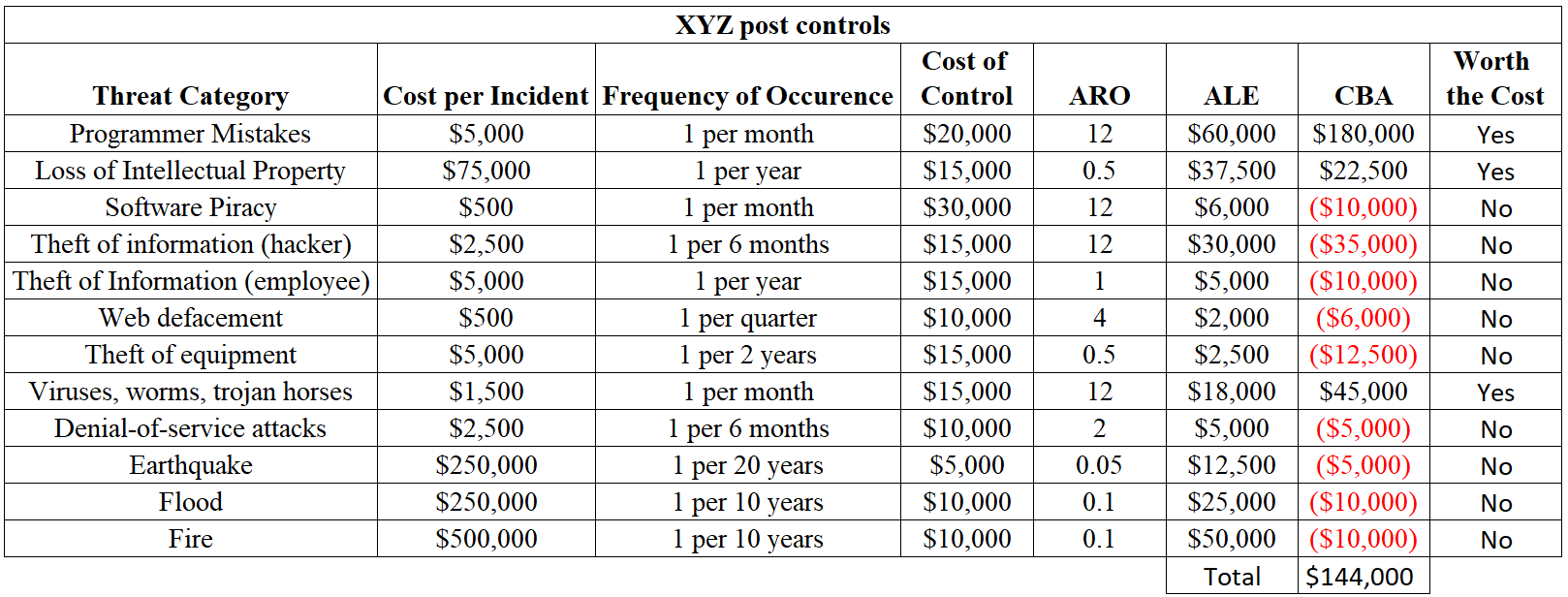
**Problem 2**

Complete Exercise 3 from p. 320 of your text. You may create a spreadsheet to support your work and paste results into a table here. Be sure to attach spreadsheet, as well, if you choose to use one. (15 pts.)



**Problem 3**

Complete Exercise 5 from p. 321 of your text. You may create a spreadsheet to support your work and paste results into a table here. Be sure to attach spreadsheet, as well, if you choose to use one. Be sure to address the questions at the end of the problem. The calculations alone are not sufficient. (20 pts.)



*The values have changed for cost per incident and frequency of occurrence due to the controls XYZ put into place. Mitigatory controls would decrease the percent of the asset lost per incident (SLE) but not necessarily how often the attacks are successful and defensive controls would lower the frequency an incident would occur (ARO) but not necessarily how damaging a successful attack will be.*

*Overall, the most useful control was training programmers to limit their mistakes. In total, implementing all controls would still make economic sense, but individually, only three categories make economic sense to implement controls for. Those are Programmer Mistakes, Loss of Intellectual Property, and Viruses, worms, trojan horses. The remainder cost more than they save and should only be implemented due to other considerations, such as regulations, laws, or if the extra expense is worth preventing a loss of reputation or customers.*